International Journal of Cyber-Security and Digital Forensics (IJCSDF) 4(1): 272-289
The Society of Digital Information and Wireless Communications, 2014 (ISSN: 2305-0012)

BYOD NETWORK: Enhancing Security through Trust–Aided Access Control Mechanisms

[1]Francis Nwebonyi Nwebonyi, and [2]Uchenna P. Daniel Ani
[1]Department of Computer Science, Ebonyi State University, Abakaliki, Ebonyi State, Nigeria.
[2]Department of Computer Science, Federal University Lokoja, Kogi State, Nigeria
[1]*francis.nwebonyi@ebsuai.edu.ng*, [2]uchenna.daniel@fulokoja.edu.ng

ABSTRACT
The growth of mobile devices both in variety and in computational abilities have given birth to a concept in the corporate world known as Bring Your Own Device (BYOD). Under this concept, Employees are allowed to bring personally owned mobile devices for official work. Though relatively new, it has gained up to 53% patronage among organisations, and it is expected to hit 88% in the near future. Its popularity is driven by significant advantages ranging from reduced cost, employee satisfaction to improved productivity. However, the concept also introduces new security challenges; for instance, the organisation looses the ownership of devices used for official work, to the employees. Implying that the employees own and manage the devices they use to work, including seeing to the security needs of such devices. With this development, protecting the corporate network becomes pertinent and even more challenging with an audacious need for outwittingconventional access control mechanisms, giving the highly dynamic nature of mobile devices. Considering the fact that BYOD is also a type of pervasive/dynamic environment, this work studies similar dynamic environments, relating to how their security challenges are addressed, and from such bases a Trust-Aided Dynamic Access Control Approach is proposed for enhancing the security of BYOD devices. Through computational analysis, this scheme has been seen to be security-compliant and could significantly improving the overall security of BYOD networks.

KEYWORDS;
BYOD Security, Access Control Security, Trust and Security, BYOD Trust, Dynamism in Security

1. INTRODUCTION
Bring-Your-Own-Device (BYOD) is an operational phenomenon that let employees bring personally owned mobile devices for official work. It has gained much acceptance amongst organizations because of the tremendous evolution in the number of mobile devices available in the market today. The BYOD concept is introducing a move from the typical approach where concerned organisations/enterprises usually owned and managed the devices used in their offices or for official tasks. In such conventional modes, organisation owned it all, and had less worries about nodes or systems connected to their network since the IT department knew about all of such devices, and checks them for security compliance. The concept shifts device ownership to the employees, introducing mobile devices in the place of the fairly stationary systems.
This trend has unveiled promising advantages ranging from cost savings relative to purchase and maintenance of organisational devices, to more employee satisfaction; since the employees are allowed to use their own devices which they are more comfortable with. The approach also promises increased productivity and efficiency stemming from the mobility capacity introduced, this enables employees to work from anywhere and at any time [1].

In spite of the promising gains of BYOD, the system yet reveals security concerns that should not be overlooked. Security is a basic issue in all pervasive computing environments [2], and BYOD is no exception. The security trepidations in question demand the attention of not just organisations, but researchers as well. A league of questions abound that exposes the dangers of employing BYOD trends in enterprise or private systems. Questions about what happens with the data and the equipment upon termination, how does one ensure prompt deployments of security updates? How are the issue surrounding licensing, ownership or access resolved? What are the scopes of security scans and how are they accomplished? What are the assumed reasonable

expectations of privacy of employees and employer alike? How do organisations appropriate monitoring and compliance to company policies and code of conducts? [3]. BYOD also bears several properties typical of other pervasive computing paradigms, which eventually have turned-out into glitches in disguise. The concepts of respecting user intents, dynamicity, context-awareness, automatic evolution, and adaptability [4], [5] in [2], are about the most important of the features that have overridden traditional security approaches. All pervasive computing user's access is not only dependent on "who user is" but also on "where the user is", "what the states of users' and environment are" and "what intents users and service providers have" " [6] in [2]. And since conventional access control mechanisms separate each of those factors, specific access control framework would be desired to meet the joint requirements of pervasive computing environments, and more specifically BYOD.

These and many more are very serious issues that reveal as much concerns as the benefits accrued in adopting the technique.

The concerns are quite dissimilar, besides, BYOD as a type of pervasive environment is characterised by inescapable mutual collaborations of mobile devices, rearing up more security issues than those experienced in conventional networks [7]. The information technology department of concerned organisations are not able to produce confident and accurate accounts of the security state of interacting nodes/systems at any given point. Such accounts are only obtainable within the luxury of devices ownership, which apparently is lost to the employees. Similarly, the shift to mobile devices also introduces renewed shortcomings. For instance, mobile devices easily collaborate with other devices outside the organisational network, thus exposing it to a higher risk of threat, and making it more difficult to securely incorporate them into a network. Furthermore, traditional access control systems are not suitable for the dynamic and mobile nature of BYOD devices and system given that they only focus on user identity or role(s) to make access permission decisions [8].

Given the difficulty of keeping track of mobile devices as they roam in and out of compliance, there rises the need for a more subtle and automated means of observing the behaviour of interacting nodes, noting the infeasibility of physical patron and inspection of the security compliance of devices. From a security perspective, a device-aware access control system is likely to enhance the security of BYOD networks. This requires the introduction of key security principles like 'Trust'. Why? Because we propose that the past behaviour of devices could be used to infer the next behaviour when it connects to the network; in order to determine if it merits a pass to the network resources or otherwise. Most desirable is a scheme that is able to ascertain the trustworthiness of interacting nodes early via trust value computation, which could then be used for access permission decision. This is aimed at securing the network resources by dictating and dropping malicious (non-trustworthy) node(s) out of the network to prevent such from causing security breaches. Though not a replacement for existing pervasive computing control systems, it is however, a way of making access permission constraints more dynamic to suit the dynamic nature of BYOD network.

Is this that important? We would come affirmative with necessary alibi. The concept of BYOD is becoming prevalent, and many organisations are shifting to it. A recent research reveals that 53% of corporate organisations have endorsed the concept of BYOD and had already begun its use [9]. The authors described it as a brand new concept, yet it has gained high level of popularity. It is envisaged that in the near future, it will spread significantly to more organisations. This tremendous growth is also emphasised in [10], where 88% of IT leaders have been presented as seeing a future in BYOD. As we know, the concept massively involves mobile devices; owned and looked after by employees. Sadly, these users are usually thoughtless about security issues. About 66% of them never use any form of antivirus or security application(s) to guard against compromise [11].

No doubt, it is rather risky for any organisation or network systems to rely on users (employees) for the security of their network just hoping that such users would always abide by laid down security policies and ethics. Thus, access control has been identified as a vital and acceptable security approach in ensuring the security of corporate network resources. Unfortunately, the conventional access control mechanisms are derisory given the dynamic nature of mobile devices involved in BYOD; and since they only base permission decisions on user identity or role(s) [8]. Other non-discretionary access control systems have also emerged which has attempted to meet the needs of some pervasive/dynamic environments with insignificant results. They are either not dynamic enough to keep track of these mobile devices as they roam in and out of compliance, or are specifically channelled for specific environments and therefore cannot fit into the security needs of BYOD.

Hence, aside from technical consciousness, there are needs for new and adaptable methodical approaches for dynamically dictating and filtering out malicious nodes from the network to enhance security. This would save the numerous organisations mass-migrating into the BYOD system from huge potential losses, knowing that just a single malicious node could jeopardize the entire network leading to loss of vital organisational resources. Solving the problems of BYOD just like any other pervasive environment requires contributions from both the academia and industries. Solutions can only be reached through in-depth research and analysis of the problem landscape and making out suitable trust-based schemes for apt screening of malicious nodes in a BYOD network.

This discourse seeks to present a device-aware access control system that intensifies BYOD security with relativity to trust. The system establishes trust amongst interacting nodes via value computation that determines access grants or denials and securing networks by admitting or dropping nodes based on computed permission. Historical behaviours of devices will be used to infer future behaviours when coming into the network, this measure would help determine if nodes merit a pass to the network resources or otherwise.

The rest of the work is organised as follows; section II takes on the review of related literatures covering the concepts of BYOD, Access Control systems, trust and applications to BYOD. Sections III presents the logic behind our proposed approach giving the outcome of computed results and analysis. Section IV covers the conclusions and future work areas.

2. BYOD CONCEPT: REVIEW OF RELATED WORKS

BYOD though seemingly new has attracted the attention of researchers in a broader scale [12]. The additional security vulnerabilities created by attendant mobile devices makes for the huge research interest tending towards BYOD. Such ambiguities arise due to the mobility state and limited resources of devices, which make them more susceptible to attack. The author of [10] placed these attacks under four major classes, maintaining that users also constitute attack vectors given that a vast number of them are not able to use common security mechanisms. The argument is that any network system which entrusts reasonable security responsibilities on the employees (users) need to ensure adequate approaches to fend for potential threats that may arise even from the users.

Similarly, a research work [13] was dedicated to the challenges arising from mobile devices, particularly in BYOD. The challenges were classified as follows; Physical risk (resulting from theft of devices), Access risk (resulting from uncontrolled access by devices), usage risk (as a result of collaboration with other devices and applications) and memory risk (acknowledging the limited resources of mobile devices). An earlier work noted trust to be strategic in addressing the challenges of BYOD-based network. It pointed out that mobile devices are self-motivating in nature and demand a dynamic approach for their monitoring, as they roam in and out of compliance [14]. In our work, we capitalise on trust to derive

an access control scheme through which some or most of the problems identified above could be addressed, specifically the Access risk.

The authors in [15] worried about the wide gap between computational capabilities of mobile devices and the security provisions in their operating systems; stressing that a good number of security breaches arise from some malicious applications which the users may install. They therefore proposed a BYOD security framework to sieve applications that users can install on their devices, by such, forbidding any application that does not comply to the security requirements from being installed. Though an admirable improvement from earlier works that just suggested the problems; the scheme still bore limitations. It should be understood that not all threats encountered by mobile devices come as a result of installing known malicious applications. The mere engagement of a device to some form of collaboration with other devices can get it infected with malware and viruses, which could even be more dangerous than known malicious applications. Thus, the security framework only proffers a partial solution to the alarming security concerns of deploying BYOD.

2.1 Access Control Schemes in BYOD and Other Pervasive Computing Environments

Several works have emerged targeting the control of access to mobile and pervasive computing environments. CASA framework was proposed by [16] based on RBAC for pervasive computing environments. The CASA framework controls accesses only based on the context of being invisible. However, other essential contextual properties of pervasive computing devices such as respecting user intents, heterogeneity, and dynamicity are not covered. Javanmardi et al. in [17] projected an access control framework for Pervasive Computing Environments which handles some of the weaknesses of earlier frameworks. The framework covers some key requirements such as context-awareness, invisibility, and respecting user intents. It however overlooks pervasive computing properties of high heterogeneity and dynamicity. This loophole was further taken care of in [2], where they proposed an access control framework that addresses among other properties, the aspects of heterogeneity and dynamicity of pervasive computing environments. The framework was noted to be adaptable and dynamic based on context changes in the environment.

In [18], a solution was proffered for securing BYOD systems using Network Access Control mechanism. The approach highlighted how a large financial service organization utilized Network Access Control (NAC) and mobile device management (MDM) solutions to establish policies for enabling a bring-your-own-device (BYOD) environment with an acceptable level of risk. The system was an extension of an already deployed and working NAC policy setup for corporate-owned and managed Windows devices based on proprietary solutions of ForeScout [19], enforced policies and commands on Cisco network infrastructures. With the success recorded in the management of BYOD devices the authors noted that combination of NAC and MDM can support a flexible BYOD environment with an acceptable level of risk for many organizations. NAC could help check for the presence of an MDM agent for unrestricted access, while endpoints that do not have the agent can be blocked or granted restricted access (for example, Internet access only). Such systems could manage and ensure employee compliance to policies if they wish to gain access to the corporate network. Building automated operational processes is key to scaling a BYOD project. However, there are some reservations with this system. Little consideration is given to the vulnerability states of the nodes and how such should or could influence access to the network.

The authors in [20] propose a safe certification and authentication model for mobile internet users to control household devices safely. The proposed structure promises considerable shift drift from conventional weighty certification structures like PKI, and minimizes encryption and decryption operations by compounding session key and public key. Results from a test simulation of the model on an IEEE 802.11 wireless network shows

significant drop in the times for encryption and decryption operation to half and extends operation time to twice by managing the registration during hand-off. This it achieves using session keys that simplify accessibility for lower computing capacity mobile device [20] . A privacy-enhanced anonymous authentication and access control scheme for secured interactions between mobile users and services in pervasive computing environments (PCEs) is proposed in [21]. The framework offers an optional context authentication capability (user location). It seamlessly integrates blind signature with hash chain to achieve an exceedingly flexible and light weight authentication and key establishment protocol that is DoS resilient. Key features of the model are mutual authentication and anonymous interaction. A mechanism for the enhancement of authentication and credentials management in mobile agent environment is proposed by [22] **.** Their approaches leverages on trusted computing platform as base-platform for running mobile agent systems, and the trusted platform module is used to aid authentication and credentials management. In the long run, the security of mobile agent is improved using the trusted computing platform which is linked with upper layer applications through the trusted software stack [22]**.**

Researchers have also developed RBAC models precisely meeting the needs of context-aware pervasive computing applications [23], [24] in [25]. Gaia [23] in [25] outlines three dissimilar role categories; system-wide roles, active space roles, and application roles, and a connection between them. The GRBAC model [16] in [25] considered context information as the environmental role, which an application needs to retain in order to accomplish context-dependent tasks. It is noted that such a definition leads to large number of roles in an access control system, as there might be potentially many environmental states that are relevant for an application [25].

A context-aware RBAC (CARBAC) model for pervasive computing applications is presented in [25] which is driven by context-based access control requirements related to users' memberships in roles, permission executions by role members, and context-based dynamic integration of services in the environment with an application. The Context information form basis for role admission policies [25] . From the results from experimental test beds, the models proves useful for managing access control in pervasive computing environments with fascinating features like support for personalized permissions for role members, context-based constraint specification as part of - dynamic binding of objects with active space services, user admission to roles, permission executions by role members, and granting access to a subset of a service's [25]. A Spatial Role-based Access Control (SRBAC) model is also introduced [26],which is an extension to an earlier model. The model manages access controls based on role restrictions and access decision requirements derived from the spatial dimensions in which the user (his/her mobile device) is located; to enable the restriction of resources access to limited locations as necessitated by the system requirements. The model which permits location-based definition of security policy has unveiled a notable desirable requirement necessary in future mobile computing platform [26].

A shared resource access language, SRAL, is proposed [27] to model mobile device behaviours of habitual relocations among diverse networks and connecting to different data servers at different times. The language is structured and compositional such that mobile applications can be constructed recursively from primitive accesses. The SRAL model also takes abstractions from conventional role-based access control (RBAC) model to specify and enforce spatio-temporal constraints. This is achieved using mathematical computations in polynomial-time algorithm [27].

Like pointed earlier, the main function of access control is to regulate access to system resources and to mitigate related vulnerabilities. Risk-Aware RBAC [28]is also introduced; whose access permission decision is based on estimated risk, as opposed to the traditional RBAC system where access permission decision is based on pre-

computed policies which returns same result always. This creates a new form of dynamism. A session risk threshold is used to check the number of roles that could be activated by any user at any given time, so as to keep watch at the level of damage that could be caused on the network assuming the user begins to act malicious. This approach sees the introduction of an intelligent agent monitoring the interaction of users and updating the system on such interactions; triggering off when the risk threshold is exceeded within the session.

Though excluding trust, this model projects a bit of the idea for which our work is based. Such ideas include dynamic elimination of malicious nodes from the network based on a threshold, to save it from further potential harm. Nevertheless, the system flaws in its reactive nature, only able to halt already started malicious activity. A clear cut prevention from start-up would be a better solutions. Additionally, only users are considered and not devices being used, discounting the fact that more threats can originate from devices rather than just users.

Apt analysis show that the mentioned approaches are hardly suited for BYODs' kind of pervasiveness. Apart from the traditional access control models which is strictly based on the identity or roles of users, and are static in operation as pointed out earlier, the attribute based systems only emphasis on the users, and nothing about the device being used. This could mean that a compromised node can access the network without any form of check; thus exposing the entire network to potential jeopardy. The risk-based approach is considerably dynamic, but it is only reactive and not proactive; meaning that it does not relate to the current behaviour of users to stop them from causing harm in the future. It only works for current sessions, added to the fact that emphasis are also on users only.

Our proposed method aims at monitoring the devices as they interact with the network, to infer malicious behaviour from past interactions, and to drop any suspected device. The benefit of this is that users are subjected to the adherence of organisational security policies not only by avoiding malicious applications as suggested in the previous approach, but also by installing recommended software such as antivirus and anti-malware applications as a way of protecting their devices from threats. This method of dynamically checking device reliability which has not been found in traditional access control systems and some other approaches is a novelty our work pursues.

2.2 Conceptualizing Trust

Trust is inevitable in human life. The occurrence of human activities works on the basis of trust, for instance, getting on a bus and trusting the driver not to run into other cars on the road, driving our own cars trusting that they are safe enough for us, and trusting that that our money is safe in the bank, among others. Trust is noted to be an unavoidable concept in security, without which adequate reasoning of the security of any system may not be conceivable [29]**.** However, there has not been a unified agreed-upon meaning for trust.

Trust could be viewed in terms of certainty and believe. More like saying if Bob trust Alice, then it implies that Bob believes that Alice is trustworthy. If a device in a network trusts another device for an interaction, it is a reflection of this human attribute (believe) that the device will not act maliciously in a way that could cause security breach. It has been strongly suggested that trust grows in proportional measure to the amount of available evidence, an assertion that trust is based on evidence of favourable experiences with a given agent. Trust also grows with time, as the number of interaction with a given device increases; more information about the device is gathered as basis for a clearer trust decision [30]. Contrary to the effects of favourable evidences, unfavourable ones can also destroy trust believe. For instance if a device is used to acting behaviourally well, and suddenly begin acting maliciously, the earlier built trust may be reversed and such devices may not be trusted anymore. This attribute of trust is referred to as dynamism.

Trust can also be viewed in-terms of probability. In [31] a direct link was established between trust and the probability of outcomes; implying that the past behavioural history of users could be used to calculate the probability of their next behaviour. Favourable past behavioural history will suggest a trust, otherwise mistrust.

For the purpose of this study, we shall go in line with [32], in which trust was expressed in-terms of probability threshold. According to the author, trust refers to a level of probability in which a party bases his/her assessment that another party will act in a particular manner, usually before monitoring such action, and in a manner that defines his/her own action. The author first introduced probability range of 0 to 1, as representation of trust; with 0 representing mistrust and 1 representing absolute trust. He further explained that for a person to trust another, it means that there is high enough probability that the second party will act in a favourable manner or at least in a manner that will not be harmful. The proposed algorithm closely relates to this in finding out beforehand whether a node will act malicious or not if allowed access into the network, and with such information determine if access will be grated or not.

1). Trust Forms

Trust can be viewed in relations to cooperation [32], commodity and reputation [33], direct and recommended trust [34]; the perspective of which comes applicable to our context (BYOD network). While recommended trust usually involves a party that has not been directly interacted with in the past, and there is no base for trust, direct trust is a kind of trust developed directly with an agent, usually as a result of past experiences [34]. Our direct trust concept involves a prior registration of employees' mobile devices as part of the criteria for initial decision on trust concerning nodes joining the network for the first time. However there is also the possibility of an unregistered device legitimately accessing the network, whose case is already noted for further recommendations. Figure 1 illustrates how direct trust can be extended among agents who are involved in interactions. As shown, A2 trusts A3 and A4, while A4 trusts A1. A1 has no trust relationship with A2 and A3 before, but as can be seen from the diagram, they now share recommended trust relationship. A4 recommended A1 for A2, while A2 further recommends it to A3.

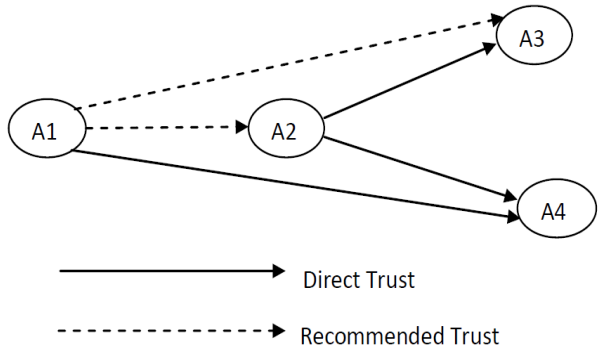


Figure 1: Representation of Direct and Recommended Trust [34]

2). Trust in other Pervasive Environments

Trust is a key principle that comes indispensible in our contextual analytics. Though said to be elusive because of the infeasibility of absolutes [35], it is still viewed as a mechanism that tends towards dropping societal complexities, and yet causing vulnerabilities towards subject or objects [36]. From a philosophical perspective, Rotter defined 'trust', specifically 'Interpersonal Trust' as expectancy held by individuals or groups that the word, promise, verbal, or written statement for another can be relied upon. He has experimentally shown that trust possesses constructive significance to operational society [37]in [36]. The world of economics views trust as a forecaster of satisfaction in organizational decision-making [36]. These principles about trust have been applied to pervasive environments just like its contemporaries before, and tremendous successes have been recorded.

For instance, e-commerce environment is one of such pervasive nature that has enjoyed a fair share of trust and its applications. This is evident in [38] where the authors identified reputation as very vital in fostering good behaviour and also encourages compliance to contract agreements in e-commerce. Similar to the real life scenario that would require some form of enforcement to foster compliance, their system introduced reputation system as a way of promoting adherence to electronic based agreements or contract, and encouraging trust in e-commerce, even among

strangers. Their stake is that without such ideas as theirs, which uses past partner transaction experience to project into the future, there would be more tendencies to act in a deceptive manner for dubious gain during e-commerce transaction involving strangers.

Vehicular network is another specific pervasive environment where trust has been dedicatedly proposed for access control and enhanced security. The Situation Aware Trust (SAT) model proposed in [39] provides for building trust among vehicles in a network. They introduced the concept of social network as a means of ensuring trust decentralization even if the vehicular network is temporarily unavailable or is facing attack. Among the novelties they introduced includes incorporating the prediction of future trust conditions into the VNET, and linking the concept of trust from the normal social internet communities to vehicular network applications.

Trust has also been introduced into online social networks as discussed in [40]**,** their concept suggests that the real life view of trust can be employed towards a more secure online social network with the likes of their proposed 'Safebook'. They presented online social network as a digital reflection of the physical relationship that exist among participants. The theory of acquiring genuine recommendations when the need arises also comes as a handy suggestion too [41].

Professional Virtual communities are a phenomenon that sprouted from social groups and online meeting. This is such that offers a platform for professional knowledge sharing without face to face contact or meeting. The authors in [42] identified that individuals not being willing to shear their knowledge is a major factor in VCs, and this willingness is a subject of expected outcome which is dependent on trust. Expected outcome in this context has to do with monetary gains or opportunities of interest which the user can trust the other party for before sharing needed information. They presented trust as an implication of a belief that a second party will act as expected, and argued that since there is no physical interactions and legal guarantees in VCs, only a trust based model can be adequate. The representation of the model as shown in the figure below, demonstrates that trust is a peak factor in knowledge sharing.

3. TRUST IN BYOD

As observed, in most pervasive domains, the client nodes are usually the ones in need of acquiring the trustworthiness of the server nodes [43]. However, this is not the case with BYOD, because, client nodes already have reasonable trust on the corporate network (server).

Conversely, we present our approach, which takes a slightly different mechanism from conventional approaches. We propose a way of enabling the corporate server in a BYOD environment ascertain the trustworthiness of any client node before unleashing service(s) to them. Our focus is on the behaviour of the devices; which is a potential contextual property, rather than just the users of the devices as seen in the earlier models. And we use the comportment of each randomly associated node to prevent potential occurrences of security breaches; instead of just reacting to current session as some of the approach discussed above suggests. Ensuing the successes of trust in the specific pervasive environments discussed, there are likelihoods that channelling trust to the specific need of BYOD will amount to a clearly more secure network implementation involving its randomly associated nodes.

Many thanks to the triple space of trust; belief (favourable outcome), disbelief (unfavourable outcome) and uncertainty (not enough grounds to decide) [31]. Although not entirely suiting our context, we abstract from their idea of not specifying exactly 1 and 0 as values for passing and dropping a node respectively, but rather use a continuous real number range from 0 to 1, with specification on minimum threshold. This allows for devices to be granted access even without an absolute trust value of 1, provided the threshold is attained; since no device can be 100% trusted.

We also take an excerpt from [44] whose ideas projects the concept of 'effect of evidence' and 'effect of conflict' in the computation of the

expected trust values of each returning randomly associated node. Effect of evidence suggests that an increase in evidence result to an increase in certainty of trust, while effect of conflict suggests that conflict in evidence decreases certainty of trust. Sticking that to our approach, the favourable behaviour of any randomly associated node represents the 'effect of evidence', while malicious behaviour of such nodes denotes the *'effect of conflict'*. In [45] and [8], the alpha beta probability concept have been presented as a competent means of predicting future occurrences from past experiences. We agree with their proposition and base our notion on the beta (β) distribution expressed as follows:

$$f(p|\alpha,\beta) = \frac{\gamma(\alpha+\beta)}{\gamma(\alpha)\gamma(\beta)} p^{\alpha-1}(1-p)^{\beta-1} \quad (Eqn\ 1)$$

Where $0 \leq p \leq 1$, $\alpha > 0$, and $\beta > 0$.

With the constraint of the probability variable (p) not being 0 ($p \neq 0$) or being 1 ($p \neq 1$) when $\alpha < 1$ or $\beta < 1$ respectively, the expression for deriving the expected value of beta distribution from the known value is given as;

$$E(p) = \frac{\alpha}{\alpha+\beta} \quad \_\_\_(Eqn\ 2)$$

As expressed in the next chapter, we redefined α and β to suit the requirements of our system without actually violating any mathematical orders.

4. TRUST-AIDED DYNAMIC ACCESS CONTROLAPPROACH (T-ADACA) CONCEPT

Our Trust-Aided Dynamic Access Control Approach (T-ADACA) takes base from Probability Density Function (PDF), a scheme that helps in conjecturing the future actions of individuals from their past interactions. This approach of looking-out for the future has seen tremendous patronage in various dynamic environments, especially in e-commerce. We also key into this measure towards deducing the prospects for safe or unsafe interactions amongst BYOD nodes. The probability of safe interaction is termed trust, while the possibility of unsafe interaction is tagged mistrust. The Approach introduced defines a conceptual framework that could be applied to prevent potentially malicious (mistrusted) nodes from accessing the network, while allowing only the potentially safe (trusted) nodes. Through this means, the network can be kept free from threats originating from malicious devices; thus enhancing the security level of the network.

Adequate network security may be difficult (if not impossible) to achieve without suitable access control scheme. It is a core security need because if access is not restricted in any way, then any user through any means can exploit the system. Consequently, the proposed framework relates to the always available, conventional and human way of trust and access control; to introduce adequately a dynamic access control approach for organisational networks which are BYOD-based. The previous interaction history of the node is used to compute its trust status, which is further used for access permission decision.

In non-technical terms, we only open our doors or give our keys to trusted personalities. Such trust may have been built up through prior direct interactions or trusted recommendations. We employ this natural tool, without ignoring the fact that trust does not equal security (Trust ≠ Security), but also acknowledging the close relationship between trust and security.This close relationship between security and trust propels our motivation. Fig 2 shows the flowchart of the proposed T-ADACA System.

We refer to the whole T-ADACA process framework as trust engine. It starts by retrieving the interaction history of each node as it attempts accessing sensitive resources in the network. Using the information from the interaction history of the device which is already stored, the expected behaviour could be calculated based on probability. The number of favourable interactions is represented by H_f while that of the unfavourable (malicious) interaction is represented by H_u. Our model works on the assumption that there exists an intelligent system that keeps track of the

behaviour of the nodes, and feeds the trust engine with necessary information. Such intelligent agent watches out for various forms of threat, especially the ones that lead to privilege escalations; causing a node to access information which is not meant for it..

4.1 MATHEMATICAL REPRESENTATION

Most trust model present recommendations as a way of building initial trust for first time users. However, the BYOD terrain suggests most attentions to be usually focused on the employees; bringing their own devices to work and using them for official functions. We assert that for an individual to be an employee in any organisation there has to be a kind of prior contact, not necessarily with the network, but obviously with the organisation. If so, then such employee is also bound to observe the policies of the organisation. This is applicable to both first time device users and returning device users.

1). First Time Devices

Access decision for first time devices are based on policy compliance such as the ones outlined earlier, after which the interaction history will be maintained and used for subsequent access decisions. An ignorance value expressed as $R \in \{0, T_{min}\}$ is assigned to a first time device which has no previous interaction history with the network. The value to be assigned will be based on compliance with the organisational policies on; device registration, approved device type, and operating system version. We see T_v to take a value range represented as;

$$T_v = \begin{cases} T_{min} \\ 0 \end{cases} \quad 0 \leq T_v \leq T_{min}$$

If for instance a new employee arrives an organisation and have not used the organisation network resources previously; then, adequately fulfilling these conditions will determine if access will be granted or denied. If the device meets up with the security requirements which shall be automatically checked on attempt to access network resources, then an initial trust value that is equal to the minimum threshold ($T_v = T_{min}$) will be assigned to allow it access to the network for the first time. However if the policies are not adequately met, a value less than the threshold ($T_v < T_{min}$) will be assigned to it; usually 0, thus disqualifying it access to the network.

2). Returning Devices

For devices that already have previous interactions with the network, beta distribution concept is used to determine the probability of its next behaviour, to predict safe or unsafe devices beforehand. An interaction history is usually maintained by frequent update of the number of previous favourable and unfavourable interactions. We denote the number of favourable interactions of a given device with H_f, and that of unfavourable interactions with H_u. We define unfavourable interaction as that in which the assumed intelligent system reports a malicious activity concerning a device; here, $H_u = H_u + +$. If on the contrary, a device interacts with the network without being reported until its interaction at that moment is over, then it is termed favourable; therefore the number of favourable interaction is updated just before it leaves the network; $H_f = H_f + +$.

Now having known the beta distribution formula; $f(p|\alpha, \beta)$ (eqn 1) and that for calculating the expected beta distribution value; $E(p)$ (Eqn 2),
We associate the number of favourable interactions to α, and the number of unfavourable interactions to β;$\alpha = H_f + 1$, and $\beta = H_u + 1$. Hence, the expected beta distribution value $E(p)$ or T_v can be expressed as thus;

$$T_v = E(p) = \frac{H_f + 1}{H_f + H_u + 2} \quad (Eqn\ 3)$$

Where H_f = the number of favourable interaction for a given device,

H_u = the number of unfavourable interaction of same device, and

T_v = the trust value of the devices

$E(p)$ = expected probability of nodes' behaviour (favourable or unfavourable (malicious)).

Note that T_v is expected, meaning that it is being calculated from the already gathered information as a probability. After the above calculation is made, and a trust value (T_v) of the node accessing the network determined, then a comparison of the T_v and the trust threshold (T_{min}) will be made. Access will be allowed if the calculated trust value is greater or equal to the trust threshold ($T_v \geq T_{min}$).

Information received from the intelligent system is used to update the interaction history of the nodes in the trust engine. Such information is kept to be used in calculating the expected behaviour when next the node attempts interacting with the network. If the probability suggests a trustworthy (or safe) behaviour, then access will be granted, else it will be denied. After each interaction with a device, the interaction history is usually updated to reflect its most recent behaviour. If the intelligent system reports malicious act, then the number of malicious interaction (H_u) for such device will be increased by one and the device will also be dropped from the network for security reason. If there is no such alert, then it will be assumed that the device have behaved favourably, and then, the number of favourable interactions (H_f) will be increased by one. The steps for retrieving the favourable and unfavourable (malicious) interaction are indicated in pseudo-codes A and B respectively of figure 3 below.

With the above functions, the number of favourable and unfavourable interactions will be retrieved and assigned to variables H_f and H_u respectively; which is subsequently used for the computation of the trust value. The next process after an exhaustive search of the interaction history is to determine if the device in question has any corresponding history information. If the list is exhausted without any matching value for H_f and/or H_u, then zero (0) will be assigned to each of them, to indicate that the device has no previous interaction with the network. This process in indicated as pseudo-code C in figure 4.

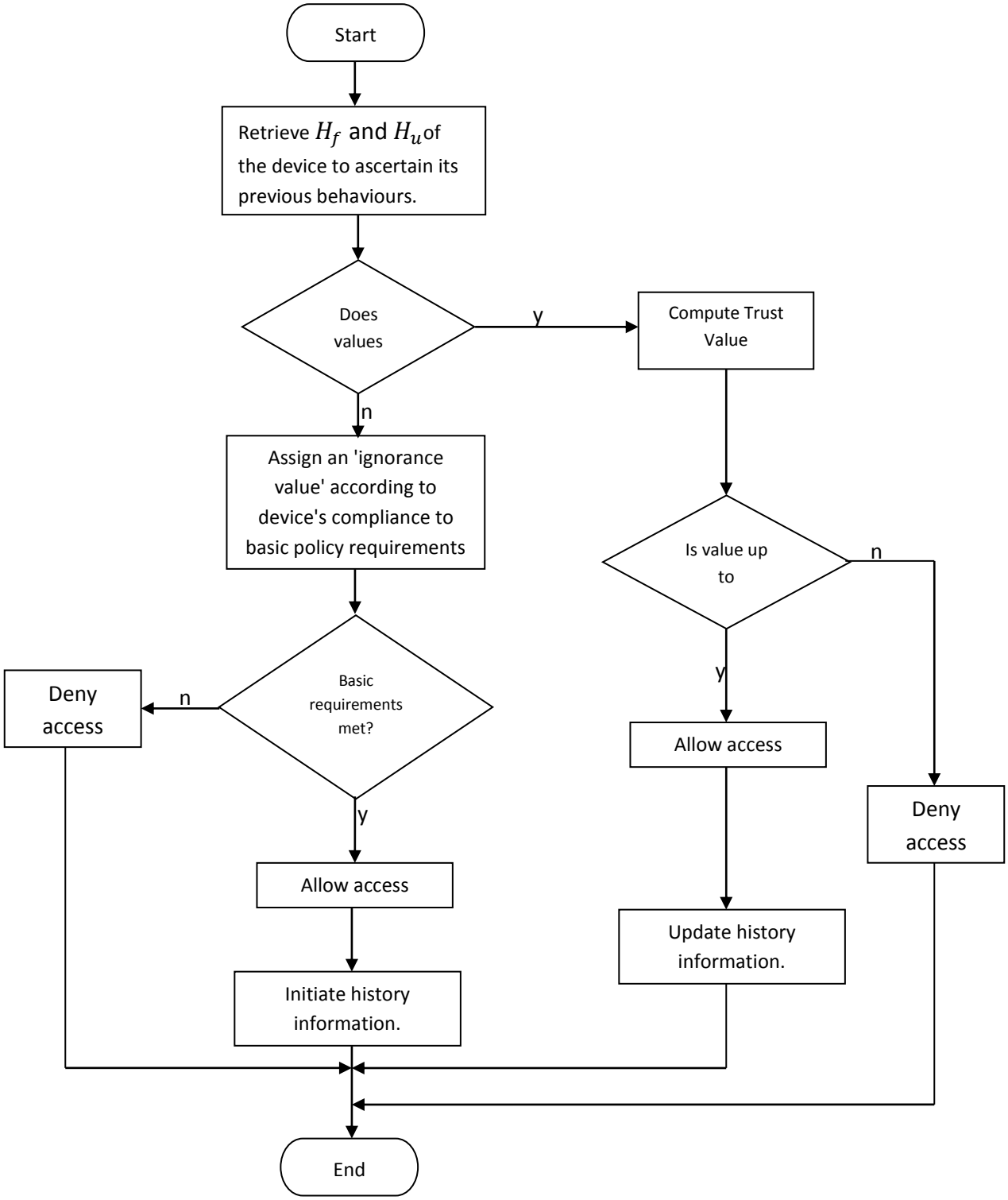
Given that the function holds (i.e. $H_f = 0$, and $H_u = 0$), it implies that the device is joining the network for the first time, in which case, an ignorance value will be assigned as its first trust value; subject to meeting up organisational specifications. Some of such specifications include; registration of the device, compliance with the device type specification, and the mode of connection to the network. If these conditions are met adequately, then a trust value which equals the trust threshold will be assigned to the node, if not, the first trust value will be assigned as zero (0); meaning a denial of access. The process is indicated as pseudo-code D in figure 4.

The variable T_v refers to trust value, while T_{min} is the trust threshold; which refers to the minimum value assigned to a first time device and documented as representing a non-malicious state. Depending on the assigned value, an access decision will be made. This process in indicated as pseudo-code E in figure 4.

Once access is granted to a node, the trust engine listens to the intelligent system for information on the behaviour of the node. If any malicious act is detected, and depending on the intensity, the device may be dropped to avoid further harm. After which the trust history of such randomly associated node is accordingly updated to reflect its most recent behaviour. This is usually done by updating the number of favourable and malicious interactions respectively. During the next access attempt by such node, the Trust value will be recalculated using the updated interaction history. The value of the probability based calculation suggests the next behaviour of the node.

However, recall that we have so far considered one of the possibilities; the other possibility is for devices that are not accessing the network for the first time, but already have interaction history with the trust engine. To calculate the trust value (T_v) which equals E(p), Equation 3 above is used. This process in indicated as pseudo-code F in figure 4.

Based on the outcome of the computation, an access decision will be made; leading to allowing or (space) denying access to the network. If a node is denied access, no further action is required of the system concerning its interaction history, but if



H_f = number of previous favourable interactions
H_u = number of previous unfavourable (malicious) interactions
y = yes
n = no

Figure 2: T-ADACA System Flowchart

A. Pseudocode (Retrieve favourable interaction)

```
1: function; retrieve favourable interaction history
2:   for all H_f ∈ (the behaviour history of nodes)
3:       if H_f is for the current node, then
4:         number of favourable interactions = H_f
5:       else
6:           keep on checking until the list is exhausted
7:       end if
8:    end for
9: end function.
```

B. Pseudocode (Retrieve unfavourable interaction)

```
1: function retrieving unfavourable interaction history
2:    for all H_u ∈ (the behaviour history of nodes)
3:      if H_u is for the current node, then
4:              number of unfavourable interactions = H_u
5:                else
6;        keep checking until the list is exhausted
7:     end if
8:   end for
9: end function
```

C. Pseudocode (Matching History Search)

```
1:  function does value exist?
2:  for all H_f and H_u belonging to the interaction history
3:    if EOF then
4:     if no history corresponds to the current device, then
5:              H_f = 0
6:              H_u = 0
7:           end if
8:        end if
9:     end for
10:   end function
```

D. Pseudocode (First Time Network Joining)

```
1:   function first time devices
2:      if device is registered, and of approved device type,
and connecting from a secure source, then
3:          T_v = T_min
4:     else
5:          T_v  = 0
4:     end if
5:   end function
```

E. Pseudocode (Access granting or Denial)

```
1:   function allow or disallow access
2:     if T_v ≥ T_min, then
3:        Allow access
4:     else
5:        deny
6:     end if
7:   end function
```

F. Pseudocode (Trust Value Computation)

```
1: function compute trust value for returning devices
2:    call "retrieving favourable interactions"
3:    call "retrieving malicious information"
4:    T_v = E(p) = (H_f + 1)/(H_f + H_u + 2)
5:   call "allow or disallow access"
6:   end function.
```

Figure 3: System Pseudocodes

the node is allowed access, it is being monitored by the intelligent system during its whole interaction, and after such interaction(s), the history will be updated accordingly.

5. RESULT AND ANALYSIS

In this section, we shall discuss the expected result of our Approach, based on the earlier explained mathematical expressions and assumption. When a device attempts access and did not comply with the basic security policies, it will be dropped and no further action will be required of the system. But if the node is granted a pass after fulfilling the set criteria, then it will be further monitored, and its behaviour history adequately updated; to be used for subsequent access permission decision.

1). Effect of favourable (secure) interactions (H_f)

Table 1 below represents the interaction history of device A, with increasing number favourable interactions (H_f). Equation (3) is used to calculate the trust value (T_v). Increase in trust value as the number of interaction increases, demonstrates that trust grows with increase in favourable (secure) interactions. If a device is separated from the network for lack of safe reputation for instance, it significantly reduces the system's exposure to potential threats, implying more security.

Table 1: Interaction History for device A with increasing favourable behaviour

Number of previous interaction	Number of previous unfavourable interactions (H_u)	Number of previous favourable interactions (H_f)	Calculated trust value (T_v)	Access Decision
2	1	1	0.5	Pass
10	1	9	0.833	Pass
20	1	19	0.909	Pass
30	1	29	0.937	Pass
40	1	39	0.952	Pass
50	1	49	0.961	Pass
60	1	59	0.967	Pass
70	1	69	0.972	Pass
80	1	79	0.975	Pass
90	1	89	0.978	Pass
100	1	99	0.980	Pass

In the graphical representation of the scenario represented as figure 4, It is notable to observe that the proportional increase of the H_f and T_v became more substantial as the number of interactions increased; implying that if a node has kept-up a safe profile for a long while, its probability of maintaining such safety profile is considerably high, and making a security decision with the consideration that it is going to act safe will most likely yield a favourable result.

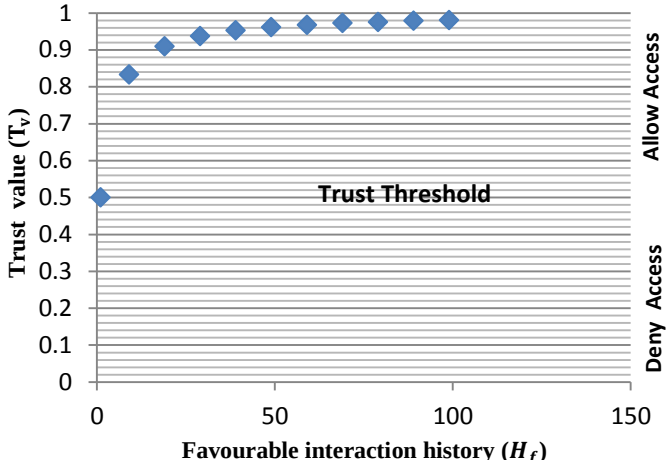


Figure 4: Effect of Favourable (secure) Interactions (H_f) on Trust Value (T_v) and Access Decision

Table 2: Interaction History for device B with increasing unfavourable (malicious) behaviour

Number of previous interaction	Number of previous unfavourable interactions (H_u)	Number of previous favourable interactions (H_f)	Calculated trust value (T_v)	Access Decision
2	1	1	0.5	Pass
10	9	1	0.1666	Deny
20	19	1	0.0909	Deny
30	29	1	0.0652	Deny
40	39	1	0.0476	Deny
50	49	1	0.0384	Deny
60	59	1	0.0322	Deny
70	69	1	0.0277	Deny
80	79	1	0.0243	Deny
90	89	1	0.0217	Deny
100	99	1	0.0196	Deny

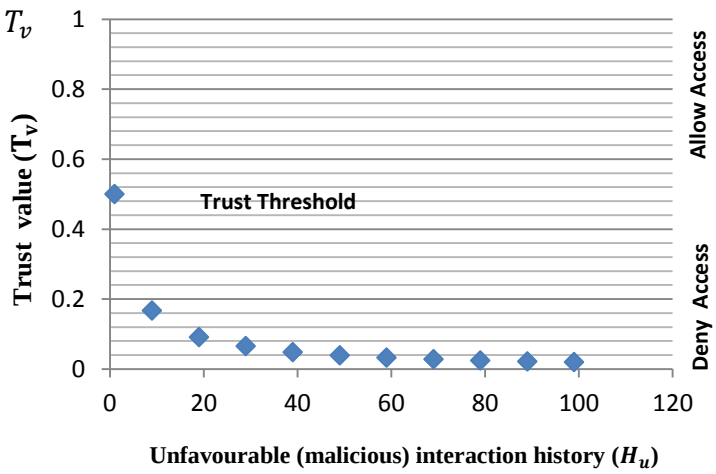


Figure 5: Effect of Unfavourable (malicious) Interactions (H_u) on Trust Value (T_v) and Access Decision

2). Effect of Unfavourable (malicious) interactions

Table 2 shows a drop in trust due to past malicious interactions of nodes. This consequently resulted to access denials to the network, to keep such nodes from threatening the entire network. A drop in trust here indicates that trust can be destroyed by malicious interactions just as the security of any system can be jeopardized by malicious activities. Indeed, trust can be destroyed even quicker than it took to build it. Equation (3) is also used for calculating the trust value (T_v) in the table.

The graphical representation of the scenario (represented as figure 5) elaborates that the more steepy slope noticed at the start of the curve illustrates that trust drops at a fast rate when a node begins to act unfavourably.

We relate trust values to the device's possibility of acting safe if allowed access to the network. The increase and decrease in trust values as illustrated with the above tables and figures also represent an increase and decrease in the possibility of devices acting safe or unsafe when access is granted to it. If devices with malicious intents are screened out of the network, then the security is surely increased, thus the aim of a more dynamic access control approach that can enhance the security of the network.

Trust and reputational approaches have been applied in a many dynamic environments but none in the form we have presented. This perhaps could be due to the relative newness of BYOD concept and the dynamic property it articulates. As noted, an earlier proposed security framework forbids a device from installing applications that do not conform to the policy of the organisation. This only takes care of threats originating from applications that have been considered unsafe. Though a good move, we consider this not dynamic enough following the roaming nature of mobile devices in and out of compliance. Even a device that did not download any incriminating application, can be corrupted by others, through mutual collaboration; thereby posing threat to the network. There is therefore a need for a more dynamic system to monitor the interactions of nodes; sieving malicious nodes out of the network and allowing the safe ones to interact.

The proposed T-ADACA framework not only discourages users (employees) from installing malicious applications to enable them maintain access to the network, but watches out for other forms of malicious activities from any connected node, acknowledging that mobile devices roam in and out of compliance easily. Malicious nodes are dropped out of the network, and a history record kept. This ensures that employees are left with no choice than avoiding all possible malicious encounters, and updating their devices with necessary applications while avoiding malicious ones so as to maintain good interaction history and consequently, uninterrupted access to the network; thus, significantly improving the over-all potential security of the network.

6. CONCLUSION AND FUTURE WORK

The dominance of mobile devices in BYOD environments speak much about its security limitations, and as organisations migrate from their usual traditional network setting towards, there is no better option than toeing the path of solution towards inherent challenges in BYOD. A

key measure is an attempt towards initiating a form of dynamic filtering for everything that enters the network; keeping the nodes with malicious intent out of the network, to stop them from threatening the entire network.

The solution proposed employs the concept of trust on the access control system to check the randomly associated nodes at their entry points; predicting those with malicious intents and denying them access to save the network from potential threats. Compared to existing BYOD model, which only prohibits the installation of malicious applications in the mobile devices without any means of checking its actual behaviour on the network, the T-ADACA approach proves more security-compliant by providing for; (i) placing a check on the devices as they access and interact with the network, (ii) keeping record of their interaction history and using it to predict the would be behaviour of the device, and (iii) blocking potentially malicious nodes from compromising the entire network.

The assumed intelligent system takes basis for future work; such BYOD-based system should be such that can sense organisational policy requirements on devices as they request access permission, and monitor the entire interaction to update the trust engine accordingly. Similarly the model can be improved by carefully making provisions for recommendations, and making out the effect of time on the interaction history, all within the scope of BYOD security requirements

7. REFERENCES

[1] S Mansfield-Devine, "Interview: BYOD and the Enterprise Network," Computer Fraud & Security, vol. 4, pp. 14-17, 2012.

[2] S Rashwand and J Mišic, "A Novel Access Control Framework for Secure Pervasive Computing," in International Wireless Communication and Mobile Computing (IWCMC), Caen, France., 2010, pp. 829-833.

[3] H Z Horbaczewski and R I Raether, "BYOD: Know the Privacy and Security issues before inviting employee-owned devices to the party," 2012, pp. 71-76.

[4] S Javanmardi, H Hemmati, and R Jalili, "An access control framework for pervasive computing environments," in IEEE International Conference on Pervasive Systems and Computing, 2006, pp. 97–103.

[5] D Garlan, D Siewiorek, A Smailagic, and P Steenkiste, "Project aura: Toward distraction-free pervasive computing," IEEE Pervasive Computing, vol. 1, no. 2, pp. 22-31, April-June 2002.

[6] F Pu, D Sun, Q Cao, H Cai, and F Yang, "Pervasive computing context access control based on uconabc model," in international conference on Intelligent Information Hiding and Multimedia Signal Processing, 2006, pp. 689–692.

[7] L Mohammed, "Towards Pervasive Computing Security," in Proceedings of the World Congress on Engineering, vol. 1, pp. 1-6, July 2-4 2008

[8] T Sun and M K Denko, "Performance evaluation of trust management in pervasive computing," in 22nd International Conference on Advanced Information Networking and Applications, AINA 2008. , 2008, pp. 386-394.

[9] A Ghosh, P K Gajar, and S Rai, "Bring your own device (BYOD): security risks and mitigating strategies," Journal of Global Research in Computer Science, vol. 4, no. 4, pp. 62-70, 2013.

[10] A Scarfo, "New security perspectives around BYOD," in Seventh International Conference on Broadband, Wireless Computing, Communication and Applications (BWCCA), 2012, pp. 446-451.

[11] M Zineddine and H Kindi, "'Smart phones: Another IT security scuffle'," in International Conference on Internet Computing , Informatics in E-Business and applied Computing (ICIEACS 2012), pp. 1-10, July 27-28 2012.

[12] M N Singh, "BYOD genie is out of the Bottle–"Devil or angel," Journal of Business Management & Social Sciences Research (JBM&SSR), pp. 1-12, 2012.

[13] F G Furtmuller, "An approach to secure mobile enterprise architectures," International Journal of Computer Science Issues, vol. 10, no. 1, pp. 1-8, 2013.

[14] MobileIron. " BYOD Strategies," Technical Report, pp 1-8, 2011. Web Tutorials, [Available Online at:] http://www.webtorials.com/main/resource/papers/mobileiron/paper1/byod_part_1.pdf

[15] A Armando, F B Kessler, G Costa, A Merlo , and L Verderame, "Bring your own device securely," in Proceedings of the 28th Annual ACM Symposium on Applied Computing (SAC '13), 2009, pp. 1852-1858..

[16] M J Covington, P Fogla, Z Zhan, and M Ahamad, "Context-aware security architecture for emerging

applications," in IEEE Annual Computer Security Applications Conference, 2002, p. 249.

[17] S Javanmardi, H Hemmati, and R Jalili, "An access control framework for pervasive computing environments," in IEEE International Conference on Pervasive Systems and Computing, 2006, pp. 97–103.

[18] L Orans, "Securing BYOD With Network Access Control, a Case Study," SANS Institute, Research Report 2012, pp. 1-8.

[19] Gil Friedrich and Chris Isbrecht, "Embracing BYOD with MDM and NAC," ForeScout, Research Report, pp. 1-30 2012.

[20] W Lee, H Cho, and J Kim, "A Fast Security Mechanism for Mobile Communication in Ubiquitous Computing," in International Conference on Convergence and Hybrid Information Technology, IEEE Computer Society, 2008, pp. 651-654.

[21] K Ren and W Lou, "Privacy-enhanced, Attack-resilient Access Control in Pervasive Computing Environments with Optional Context Authentication Capability," Mobile Network Application, no. 12, pp. 79–92, December 2006.

[22] Z Shen and X Wu, "An Improved Security Method for Mobile Agent System by Using Trusted Computing Platform," in International Conference on Intelligent Computation Technology and Automation, 2010, pp. 583-586.

[23] G Sampemane, P Naldurg, and R H Campbell, "Access control for Active Spaces," in Annual Computer Security Applications Conference (ACSAC2002), pp. 1-10 2002.

[24] M J Covington, W Long, S Srinivasan, A K Dey, M Ahamad, and G D Abowd., "Securing Context-Aware Applications Using Environment Roles," in Proceedings of the Sixth ACM Symposium on Access control Models and Technologies, 2001, pp. 10–20.

[25] D Kulkarni and A Tripathi, "Context-Aware Role-based Access Control in Pervasive Computing Systems," in ACM Symposium on Access Control Models and Technologies (SACMAT), Colorado, USA., 2008, pp. 113-122.

[26] F Hansen and V Oleshchuk, "SRBAC: A Spatial Role-Based Access Control Model for Mobile Systems," Department of Information and Communication Technology,Agder University College., Norway, Paper Report 2004, pp. 1-13

[27] S Fu and C Xu, "A Coordinated Spatio-Temporal Access Control Model for Mobile Computing in Coalition Environments," in Proceedings of the 19th IEEE International Parallel and Distributed Processing Symposium (IPDPS'05), 2005, pp. 1-8.

[28] K Z Bijon, R Krishnan, and R Sandhu, "Risk-aware RBAC sessions," Anonymous Information systems security, pp. 59-74, 2012.

[29] P Giorgini, H Mouratidis, and N Zannone, "Modelling security and trust with secure tropos," Integrating Security and Software Engineering: Advances and Future Vision, pp. 160-189, 2006.

[30] B Wang and M P Singh, "Formal trust model for multiagent systems," in Proceedings of the 20th International Joint Conference on Artificial Intelligence (IJCAI), 2007, pp. 1551-1556.

[31] A Josang, "A logic for uncertain probabilities," International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, vol. 9, no. 3, pp. 279-311, 2001.

[32] D Gambetta, "'Can we trust trust', Trust: Making and Breaking Cooperative Relations," pp. 213-237, 2000.

[33] B Parno, J M McCune, and A Perrig, "Bootstrapping trust in commodity computers," in 2010 IEEE Symposium on Security and Privacy (SP), 2010, pp. 414-429.

[34] P Lamsal, "Understanding trust and security," Finland, pp. 1-9 2001.

[35] C Lynch. (2002) Council on Library and Information Resources. [Available Online at:] http://www.clir.org/pubs/reports/pub92/lynch.html

[36] F Meixner and R Buettner, "Trust as an Integral Part for Success of Cloud Computing," in The Seventh International Conference on Internet and Web Applications and Services : ICIW 2012 , 2012, pp. 207-214.

[37] J B Rotter, "A new scale for the measurement of interpersonal trust," Journal of Personality, vol. 35, no. 4, pp. 651–665, 1967.

[38] A Josang, R Ismail, and C Boyd, "A survey of trust and reputation systems for online service provision," Decision Support Systems, vol. 43, no. 2, pp. 618-644, 2007.

[39] X Hong, D Huang, M Gerla, and Z Cao, ""Sat: Building new trust architecture for vehicular networks", ," in Proceedings of the 3rd ACM International Workshop on Mobility in the Evolving Internet Architecture (MobiArch), August 22, pp. 31-36, 2008.

[40] L A Cutillo, R Molva, and T Strufe, "Safebook: A privacy-preserving online social network leveraging on real-life trust," IEEE Communications Magazine, vol. 47, no. 12, pp. 94-101, 2009.

[41] Z Shuai, X Fen, X Yang, Y Yi-xian, and H Zheng-ming, "Trust model based on dynamic policy similarity for pervasive computing environments," in 2nd International Conference on Computer Engineering and Technology (ICCET), 2010, pp. V4-476-V4-479.

[42] M Hsu, T L Ju, C Yen, and C Chang, "Knowledge sharing behavior in virtual communities: The relationship between trust, self-efficacy, and outcome expectations," International Journal of Human-Computer Studies, vol. 65, no. 2, pp. 153-169, 2007.

[43] F G Marmol and G M Perez, "TRMSim-WSN, trust and reputation models simulator for wireless sensor networks," in IEEE International Conference on Communications, 2009. ICC'09, 2009, pp. 1-5.

[44] B Wang, C M Wong, F Wan, P U Mak, P I Mak, and M I Vai., "Gaussian mixture model based on genetic algorithm for brain-computer interface," in 3rd International Congress on Image and Signal Processing (CISP), 2010, pp. 4079-4083.

[45] W Ping and Q Jing, "A mathematical trust model in e-commerce," in International Conference on Multimedia and Ubiquitous Engineering, 2007. MUE'07, 2007, pp. 644-649.