A Secure Versatile Context Aware Framework for Pervasive Computing Environment

Alok Katiyar
Research Scholar, CSE Dept.SET
Sharda University,GNoida.
AP, IPEC,AKTU GHAZIABAD
e-mail: alok.katiyar@ipec.org.in

Dr A K Soni
Professor ,SET,
Sharda University, GNoida ,
UP , India
e-mail: aksoni50@rediffmail.com

Dr Y D S Arya
Professor, SET,
Invertis University,
Bareilly ,UP, India
e-mail: yds.arya@invertis.org

Abstract— Pervasive computing[1] imagines consistent seemless and diversion free application bolster for everyday user tasks. Accomplishing this requires a high level of computerization. In numerous situations, the reason for sensorization is setting data that can be procured unpretentiously[3] by methods for sensors. Thus, it is key to guarantee the legitimacy of the setting data, particularly, in situations where programmed choices can have extreme security suggestions. In brilliant situations, the legitimacy of setting data can be guaranteed essentially utilizing an incorporated setting stockpiling that is safely associated with every single confided in sensor. In companion based frameworks such an incorporated approach can't be connected. Rather, it is important to utilize all gadgets to circulate setting data which requires extra safety measures to guarantee its legitimacy. In this paper, we determine the prerequisites on secure setting dissemination for associate based frameworks. Moreover, we depict a nonexclusive conveyance system to empower the utilization of setting data in security basic applications. On the premise of a prototypical execution Pervasive Computing is planned to wipe out time and place boundaries by making administrations accessible to clients at whatever time and anyplace. Because of the various quantities of administrations which are accessible in inescapable conditions, the nearness of administration revelation is a need to help clients to find and use their coveted administrations.
The fundamental concentration of the review incorporates examination of the security plans regarding the utilization of security parameters, for example, setting and trust. Numerous security plans connected for different applications are considered and assessed by considering the security qualifications, for example, get to control, protection, and setting mindfulness. The review discovers setting and trust as fundamental to create versatile and precise security system. We display an assessment showing that the proposed system can accomplish an abnormal state of security that is thinking about unavoidable situations . We present an evaluation indicating that the proposed framework can achieve a high level of security that is considering pervasive environments

Keywords-Context Aware;Ttrust Management;Pervasive Computing Environment;Peer Based System,'Versatile Security

I. Introduction

A Computing history[1] began with the centralized computing and followed with Client Server Computing.,furthermore, took after with Client Server Computing ,Web Computing, and Pervasive/Ubiquitious computing applications are found to work in an open, dynamic, and adaptable condition also, have enough flexibility in choice and use of administrations whenever and put. The high impulse and heterogeneity of pervasive computing incorporate self-versatile applications[2] that are fundamental to understanding the ubiquitious computing vision of imperceptibility and universality. This nature of universality and portability require versatile security issues including protection, verification, approval, and trust. The concept of pervasive

computing was distributed by American researcher Mark Weiser in his book ""The Computer for the 21st Century" in 1991. He said in his book [1] making the Computer vanish from the eyes of the general people .In this that way individuals can't feel the nearness of computer. In the other words, one of a definitive objectives of unavoidable figuring is the acknowledgment of registering individuals situated. The fundamental contrast of unavoidable situations contrasted and the conventional ones is the propelled processing idea of individuals arranged and pervasive. In addition, benefit disclosure as fundamental process in such conditions to offer fancied administration as per clients' inclinations ought to be gone to. As specified in [2], "Benefit disclosure is the way toward finding suppliers promoting administrations that can fulfill an administration ask determined by an administration customer". Furthermore, as indicated by [3], benefit revelation is the way toward finding an appropriate benefit for a given errand. Without a doubt, the employment of administration disclosure is finding and connecting with administrations. It can be broken down into the errands of depiction, spread, determination, what's more, connection. In addition, attributable to the nature and vision of inescapable processing some major difficulties and issues exist which some of them are recorded as expressed in [4,5,6,8], for example, the broadened registering limit, adjusting nonintrusiveness what's more, security quality, setting mindfulness, protection and security issues, and portability, dynamism, and flexibility.

In this paper, we concentrate on security issues which unavoidable situations are confronted with them. In administration disclosure prepare, without considering security, everybody can abuse any accessible administrations gave by administration suppliers. In any case, some of the time, offered administrations are profitable and essential for specialist organizations and approved clients just ought to utilize them. Hence, we propose a system to bolster some security procedures, for example, confirmation and approval (as a piece of responsibility prepare) in administration disclosure to address the said issue. Along these lines, approved clients just in view of verification framework can utilize displayed administrations considering their predefined benefits as far as approval framework. To accomplish this system, the current structures identified with administration disclosure and good with inescapable registering conditions has been examined and broke down. For this situation, we have attempted to get helpful purposes of them and utilized in the proposed structure. Furthermore, for verification and approval segments, the state-of the craftsmanship arrangements which are perfect with inescapable situations are used.

The indication of this paper is organized as takes after: first of all, some foundation study of related issues is given. From that point forward, in the Area[3] as specialized center of this paper, the proposed system is examined. Taking after this, in Area[4] 4 the execution procedure of the proposed system is depicted. In the following area, related works what's more, exchange are displayed. At long last, this paper is finished up with a conclusion and future work.

[A] Prerequisites for Versatile Security

Versatile security is an accumulation of safety effort with nonstop checking to recognize or anticipate vulnerabilities hazard and represent the new surveyed threats[5] in view of the limit of the hub. The security adjustment is not another concept[6];it is the attractive quality of a framework that adjusts security in an independent way, to reply as fast and productively to seen dangers in its condition. In conjunction with the over, a versatile security is characterized as the "security arrangement/ convention that detects, takes in the adjustments in the earth, gadget limit, varieties in the system administrations with the foreseen dangers and to embrace the new security prerequisites what's more, execute itself without the interruption of the people".
To accomplish the required security in pervasive Computing what's more, related innovations, it is important to have versatile instruments/policies[7]. In the meantime, the security instrument ought to know about the setting of the gadget for calculation while playing out the investigation of the client conduct or condition. Consequently, there is a need to concentrate the examination on the versatile security by considering the defenselessness of the working setting. From[8,9] adjustments does not just mean element stacking/ substitution of programming segments or advancements yet fulfilling the prerequisites of an application adjustment. In the setting mindful frameworks, the untrusted clients additionally represent the security issues. Consequently, the security qualifications fundamentally give scope to[10] the client trust and security in setting mindful frameworks with the element of versatility. The uncovered true applications, for example, military applications, human services administration, tourism, e-business [11] shrewd spaces12,13 like - home, workplaces, college, and so on., require versatile security approaches while giving the administrations.

[B] Trust Managment

Many research works focused on the significance of setting and trust in the asset obliged universal figuring condition. The changing figuring assets, getting to administrations, system, settings, and client trust portrayed the pervasive conditions a need for setting mindful self-versatile systems[14]. Concurring to[15], the universal/inescapable figuring incorporates a complex socio-specialized framework that needs past conventional

framework driven methodologies for planning security with a all around moved toward investigation. Henceforth, we focus more on outlining the structure in view of logical and trust examination to characterize the versatile security[16,17] level in view of the prerequisite in the omnipresent condition.

In our study the security plans are put under the accompanying two classifications:
• Context based security
• Trust based security
In second, third and fourth segment examines the security plans in light of setting, trust and versatile security issues looked into with the outline and pertinent security issues. In the last area, we endeavored to condense the plans with the different research works done under setting, trust and protection issues.

II. Context based Security

This segment talks about the meaning of context, pertinence, role and versatility of the setting credit to plan security framework. The idea of setting has begun from 1990 when Mark Weiser presented the term Pervasive Computing. The Context Awareness focused towards the desktop to cell phone, physical sensors to virtual sensors and vehicular gadgets to body wear gadgets. Numerous definitions are characterized by numerous analysts, be that as it may, observed to be application particular or about to the operational condition based. We characterize the setting in the omnipresent condition as "Context as any information that is utilized to recognize, analyze, and depict the necessities and the circumstance of an element, which can be utilized to bolster the required administrations or applications".

The more noteworthy difficulties are confronted while creating systems to address security and protection issues in the setting mindful systems[18]. The setting mindful administrations raise a danger of security and protection, however an unmistakable approach keeps these dangers behind. On the conflicting, setting mindfulness upgrades the viability of the instruments by consolidating relevant information into a basic leadership process[19]. Consequently, the utilization of context[20] to give security was considered as an essential property of the universal arrange, where the administrations all the more regularly are setting mindful. From the works[16–19] done under context aware environment condition, the scientific classification of the setting for security in the universal registering condition is proposed in Figure 1. As indicated by our view, the setting can be behavioral, registering or physical. The physical settings discuss the client and natural setting like temperature, light, commotion, area, and so forth. The computational setting considers the computational assignment like limit, correspondence overhead, and related handling overhead. The behavioral setting is about area, time, circumstance, chance administration, and movement going to versatile or nonadaptive nature. Using the specific situation, another approach called, "context based security" was proposed21 through setting approaches. The new security arrangements can be set to recognize the upheld instrument for the new situation. Accordingly, the security approaches in view of setting gets on suitable component to authorize the required level of security for the current or future circumstances. In the accompanying subsections, we talk about a portion of the order that suited in the setting mindful security approaches in the pervasive computing condition.

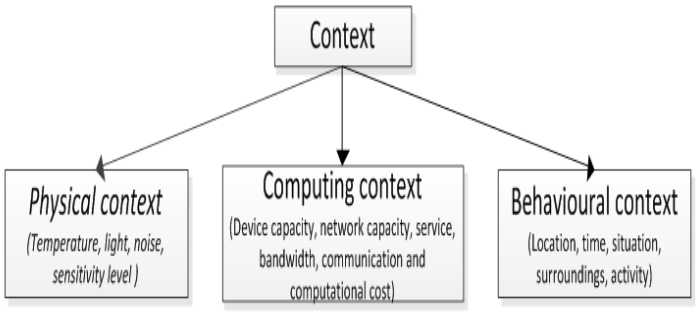

Figure 1. Scientific categorization of Context

[A} Versatile Nature in Context based Security

The possibility of versatile and pervasive frameworks is as of now a subject of extraordinary research for quite a long while to acknowledge setting data as protected innovation while upholding the security[16]. The advances developed these days empower clients to get to administrations utilizing numerous channels. In spite of the fact that the vast majority of the channels guarantee secure correspondence, it is not surprising for all intents and purposes. Consequently, a very much oversaw setting mindful security portrayal to administration get to by adaptivity and multichannel get to is much concentrated The adjustment incorporates setting lifecycle approach

and we characterized our own particular setting life cycle in Diagram 2 with the associate review[16,17]

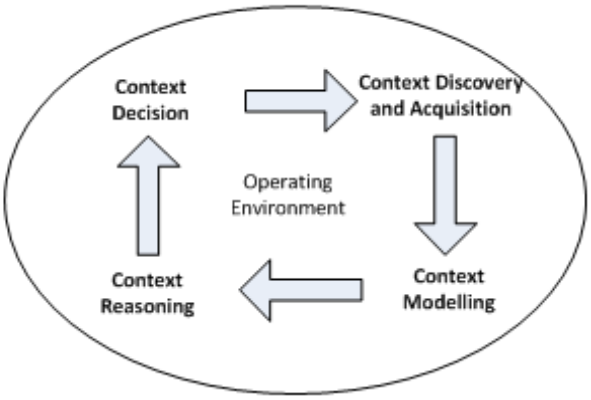

Diagram 2. Context life cycle.

Setting disclosure and obtaining incorporates revelation of the new setting in the working condition and after that to secure for demonstrating. The securing methods incorporate force and push strategy, through sensors, and sources. The methodology of obtaining change from application to application, in any case, the obtaining information continues as before. The specific situation displaying be founded on the static polices or versatile arrangements. Ideally for heterogeneous condition, versatile setting displaying strategies are most requested and are our theme of concern. The setting thinking assesses the result of the demonstrating done in light of ontology[6], graphical[12], protest based, increase dialect plans, and so forth. These thinking are supportive for setting choice. The setting choices are in the last phase of lifecycle that lingerie the substance to adjust precise choice.

While doing setting obtaining, demonstrating, and thinking, a care is expected to give security and protection. A all around characterized security conventions ensure and spare the unique circumstance. A few research works focus on giving the security what's more, protection for setting mindful applications in light of arrangement, substance, profiles, rules, and so on., yet the setting choice in setting mindful security applications need to get it the prerequisites and requests of the circumstance without the interruption of the human to arrange and structure the element operability of its inward segments. Many works slack to incorporate adaptivity, henceforth the thought of setting life cycle while planning may understanding adaptivity. In the underneath works we audit the versatile

[B] Communication and Energy Utilization Overhead in Context based Security

The protest arranged middleware encouraged the context sensitive correspondence in universal computing[23].The utilization of expansive measure of vitality, non-interoperability among reconfigurable articles and non-versatile operability for incessant setting changes progressively makes the proposition made to dally towards vitality utilization overhead. A setting touchy correspondence for administration disclosure based on metaphysics for extensive scale universal system to bolster versatile semantic inquiries with low correspondence overhead was proposed[24]. Setting delicate correspondence what's more, data apparatuses were produced and tested25 for less demanding usage, upkeep, to bolster diverse sorts of terminals, systems, and administrations, security and ease of use prerequisites. For the potential use of the portable terminal, the security concerns and dealing with the client interface requires exactness with every application. Our past work focused on vitality proficient versatile

setting mindful get to control outline for getting to the web in a unified approach[26]. The way of adaptivity was actualized based the action done in the history, sort of administration asked for, time, area and reason Contradictory[27] proposed setting mindful get to control design to secure web benefit utilizing condition parts played by the client. Both the work was an endeavor to give flexibility least calculation vitality. The catching of significant security setting of nature with least vitality will make the models more material in any registering condition. Subsequently, a setting mindful versatile, vitality proficient model was in need to outline the security structure.

[C] RISK MANAGEMENT IN CONTEXT BASED SECURITY

A theoretical model, which is a range of modeling[3,4] distinguishes the security setting and takes related social perspectives into record through an arrangement of fitting shallow level of reflection. Applied models34 were not promising towards the security administration to the new security strategies and hazard administration. Other than verification that's more, approval security issues, a danger of protection issue is brought up in the setting mindful security plans. In this respect, a protection safeguarding security challenges for a portable client were addressed35 in setting mindful versatile security structure through judging and adjusting the setting data by security control measures. Here, portable applications are executed through hatcheries to control the correspondence between the application and the gadget assets worked through an independent application.
An Explanatory Progression Handle (AHP) organized to assess the exposure of client setting (area, time, action, and so forth.,) by giving the hazard level and recommending the suitable security control choice. A comparative way to deal with give security, in view of setting was proposed[26] about the consideration of trust ascribes to limit the danger of the get to control choices.

III. Trust based Security

In this section, we discuss the definitions, taxonomy and need of trust in designing the security scheme. need of trust in outlining the security plot. The major audit was focused on the plan issues on vitality effective trust assessment and adaptivity in building up the security structure.

The trust has impacted in many controls of context systems. Be that as it may, the carelessness or nonappearance of trust brought about the postponed benefit get to, correspondence, and business reckoning. Subsequently, trust is utilized as one of the security parameter while giving the administration access in the universal systems. As trust is subjective, it is related with the physical and advanced setting while assessing. In the meantime, the fitting trust assessment choices in the pervasive system smother or stay away from the hazard components related with the conniving elements. Henceforth, a all around composed and appropriative trust assessment model is important to conquer the security hazard in the UCE.

Theoretically, trust is a parameter, used to trade data in regards to the substances activities through conviction and confidence. The conviction or confidence propels through a progression of cooperations done after some time. Cooperations might be immediate or backhanded.

In the omnipresent condition, positive practices increment the trust, and negative practices diminish the trust upon the element. Numerous specialists arranged the trust into confirmations and indicators [22,27]. The verifications are affirmed data (character, property and approval) issued by the confirmation expert or, on the other hand from other focal controlled frameworks. While pointers are conceivable components put away inside or remotely gathered from different sources39. In trust assessment, the markers are important clues when accreditation expert does not exist. Pointers are subdivided into notorieties, encounter and suggestions worried to the working universal natural context40. Subsequently, analysts concentrated to incorporate trust while building up the security plans. Numerous analysts have specified that the accessibility of reliable hubs, comprehend the security challenges in the network[41]. Subsequently, trust based security is required instead of standard validation and get to control. By including more noteworthy adaptability in outlining strategies, trust gives more control over getting to administrations and data. Consequently, the contribution of trust assessment and administration in giving security about the setting mindful installed in the security system[42]. Subsequently, trust is considered as another examination attributes[43] in the field of versatile security. The assessed trust levels are used for choice making[44] in keen situations. In addition, trust is not characterized once and proceeded

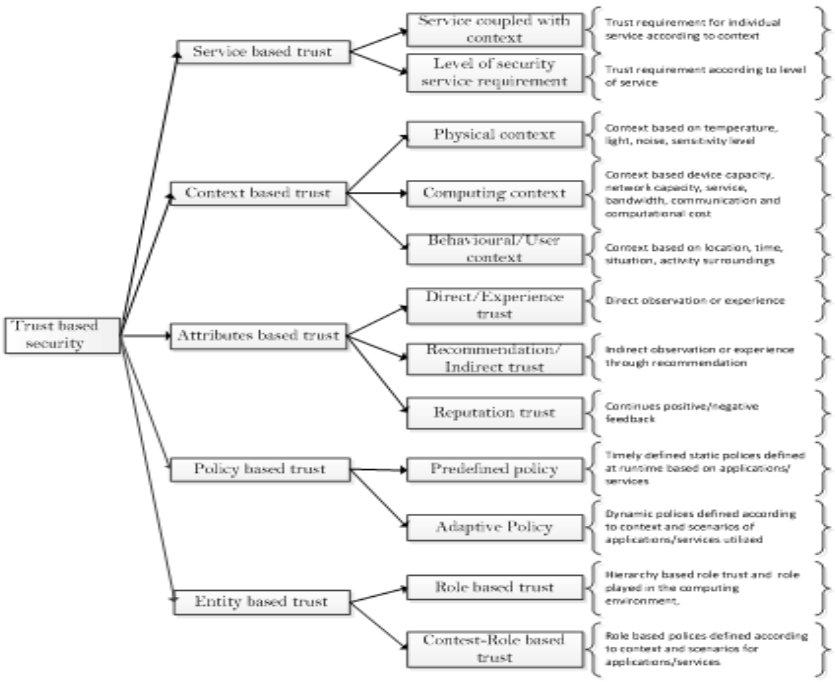

Figure 3: Scientific categorization of trust.

[A] TRUST ASSESSMENT AND POLICY BASED TRUST SECURITY

The joining of trust[23] broadened the security framework by outlining the arrangements and control over getting to
administrations/data. The utilization of metaphysics based approaches is relegated progressively or made to the new part by presenting the trust consider. These systems can deal with just when the trusted party knows the clients in the same working condition. However, the earth is most certainly not ready to present a portion of the variables, for example, • how trust is assessed
• how much trust is required and
• how much get to control is conceivable.

[B] ENERGY EFFICIENT TRUST SECURITY

The trust assessment devours a considerable measure of vitality as; it is most certainly not assessed once and utilized until the end of time. Subsequently, any model of its kind expends more vitality with regards to versatile trust assessment for security plan. In such manner, a few of the plans were audited and discovered some intriguing components to be embraced about the trust evaluation and usage while building up the security structure.
A model creating the trust self-governingly by classification of trust level is proposed49 to lessen the computational preparing time. Be that as it may, it requires a concentrated and manual organization to lessen the calculations. Consequently, usage of fluffy numeric qualities is expected while calculation, correspondence, and capacity by removing the setting of the portable clients. To work in various areas an expansive sum of capacity and the computational memory turned into a noteworthy issue. An idea of grouped systems as a spine and a portable
operator framework to accomplish negligible overhead with respect to extra messages was endeavored

[C] Adaptivity in Trust Security

Another idea of versatile trust structure was developed[25] to give security in asset obliged condition by keeping the limit and administration offered in the universal arrange. The versatile trust incorporates the determination of trust qualities (immediate, backhanded, setting, preference and social) as indicated by the kind of administration asked for and on the accessible assets in the gadget. The work was versatile towards the trust trait determination for security yet neglected to fuse confide in assessment. The greater part of the versatile trust models focus on vitality productive models rather than distinguishing the unapproved substances. In this sense, a

lightweight trust based confirmation protocol[21] had a potential to shield the elements from the pernicious assaults by fusing the trust show into modest cell phones with restricted assets and data transfer capacity.

[D] Adaptivity in Trust Security

Another idea of versatile trust structure was developed[21] to give security in asset obliged condition by keeping the limit and administration offered in the universal arrange. The versatile trust incorporates the determination of trust qualities (immediate, backhanded, setting, preference and social) as indicated by the kind of administration asked for and on the accessible assets in the gadget. The work was versatile towards the trust trait determination for security yet neglected to fuse confide in assessment. The greater part of the versatile trust models focus on vitality productive models rather than distinguishing the unapproved substances. In this sense, a lightweight trust based confirmation protocol[22] had a potential to shield the elements from the pernicious assaults by fusing the trust show into modest cell phones with restricted assets and data transfer capacity.

[E] Summary of Trust based Security

The author suggest some knowledge towards different parts of trust calculation while planning the versatile security in light of trust. We recorded a portion of the accompanying discoveries while building up the versatile security:

• Proper trust calculation/assessment through important confide in qualities, ideally (Direct trust, Suggestion Trust, Social Trust, Prejudice Trust,Setting Trust)

- Categorization of trust levels as per the security necessity.
- Methodologies to overcome phishing and malevolent substance assaults while trust calculation
- Versatile Security Schemes in view of Context and Trust for Ubiquitous Computing Environment:

A Comprehensive Survey daptive nature with vitality proficiency in the asset obliged and progressively evolving condition. At the result, a trust-based security composed with a
reasonable trust assessment display in the decentralized universal registering condition was the principal decision. At that point calculation and use of trust are viewed as based on the accessible limit and administration is a setting mindful approach towards security

IV Audit Summary of the Versatile Security in Context , Trust based Security Framework

Versatile security arrangements are intended to guarantee a high level of validation, fine-grained components for approval, sensibility to outer and interior impediments to security (e.g., limit of the figuring asset, speed, calculations) and capacity to manage irregular conditions (e.g., requirement for uncommon medicines to crises). The versatile characteristics55–58 incorporate - reaction time, viability, adaptability, heartiness and self-blemished model to mirror the adjustments progressively applications.

The incorporation of setting and trust will make the new versatile security system more dependable to the today evolving
what's more, heterogeneous condition. By considering these components, we propose scientific classification in Figure 4 that speaks to the security properties towards versatile qualities. The adaptivity can be accomplished either utilizing relevant data's or
through trust calculate. In any case, the blend of setting and trust will make the security structure more versatile and productive
At last, we firmly mean to outline the versatile security structure in light of the accompanying adjustments appropriate for the heterogeneous system, for example, the omnipresent, inescapable and portable systems.

- Incorporation of self-versatile nature in the working what's more, registering condition.
- Adaptive administration get to technique in light of the setting and trust properties.
- A legitimate nonstop checking, arrangement, examining is required to more noteworthy the new appropriate security arrangement arranging and execution of the same for administrations, applications and gadgets are required

Table 1: Commitment of research work to security

S.No	Approach	Miniature	Utilization
1	Ontology based adaptive security	Case study modeling	Smart space environment
2	Dynamic Context analysis	Context based self-adaptive	Application level
3	Trust based key generation and distribution	Security protocol model	Application level
4	Static policy and trust based	Intelligent application environment	Application level
5	Policy and trust based	Real-time application model& e-business application level	E-business application level implementation
6	Multi trust based algorithm	Estimation of trust value	MANET Application
7	Role-based and risk-aware	Specific model	Medical Information System.
8	User-centric system model	Table-lookup analysis methodology (sensitivity and cost)	Web applications
9	Trust model .	Simulation model	Service trust application for Android phones

Table 2 Commitment of research work regarding security Qualities

S. No	Access Method	Trust	Context Awareness	Privacy	Versatile Security
1	Yes	No	Yes	No	PA
2	Yes	No	Yes	P	A
3	Yes	Yes	No	No	PA
4	Yes	Yes	No	No	NA
5	Yes	Yes	No	No	PA
6	No	Yes	P	N	PA
7	Yes	No	Yes	No	PA
8	Yes	Yes	No	No	PA
9	Yes	Yes	No	No	PA

In Table 1 abridged every one of the elements with the execution furthermore, application utilization of the examination work in the last segment. In Table 2 gives the audit rundown of security investigation in view of the get to control operation executing both Authentication and auhorizaton.Subsequently, last two segments of the managed with the security conservation consider and the way to deal with give versatile security. A portion of the documentations are utilized to confirm the for researhers to calculates the Table 1 and Table 2. In such

manner, the get to control, trust, setting, and protection are spoken to with the idea of YES-for consideration, NO-for not considering the security characteristics and P-for fractional. The versatile component is
spoken to as - A, non-versatile as - NA, halfway versatile as-PA and not pertinent as-NA is considered as documentations for the versatile security worldview approaches. To finish the review, the security issues28,23,25,59–61 were unequivocally considered as the setting related and setting free components. Remembering the examination work2,26,62,63 are versatile for the dynamic changes in the adjustment of working either to inward or, then again outer setting.

V. Conclusion

Security and trust have been a test for omnipresent registering from the earliest starting point. The setting gives the significant comprehend of the circumstance or information yet increments the security dangers because of conceivable abuse of personality, area, movement, and conduct. Despite the fact that security issues are tended to at the setting mindful applications level, it is simply not went to in the setting mindful middleware level. Subsequently, security assurance necessities should be deliberately tended to by the fuse of trust. The assessment of trust and use of trust in setting mindful applications are in of essential issues. This review directed numerous arrangements toward couple with security issues. The arrangements that are more suitable to the today's reality have been talked about here with numerous security and usage accreditations. On the generally, the flexibility gives a free stage towards numerous security qualities like authentication[26], approval and get to control related with different heterogeneity parameters to guarantee the security in the universal system. Taking everything into account, security based on trust and setting set a solid base for versatile The organizing the versatile trust properties with the relevant data builds up a versatile security system that can demonstration likewise to the powerfully evolving condition.

6. References

[1] M. Weiser, “Hot topics-ubiquitous computing”, Computer, 1993, 26 (10):71–72.
[2] Patel A, Nordin R, Al-Haiqi A. Beyond ubiquitous computing: The Malaysian honeybee project for innovative digital economy. Computer Standards and Interfaces. 2014; 36(5):844–854.
[3] Lee K, Lee D, Hyun S J. A self-adaptation model for Ubiquitous computing application. Korea Advanced Institute of Science and Technology. Daejeon, Korea; 2010.
[4] He R, Lacoste M. Applying component-based design to self-protection of ubiquitous systems. Proceedings of the 3rd ACM workshop on Software engineering for pervasive services, ACM; 2008. p. 9–14.
[5] Pasquale L, Ghezzi C, Menghi C, Tsigkanos C, Nuseibeh B. Topology aware adaptive security. Proceedings of the 9th International Symposium on Software Engineering for Adaptive and Self-Managing Systems, ACM; 2014. p. 43–8.
[6] Liang Q, Cheng X. Kups: Knowledge-based Ubiquitous and Persistent Sensor networks for threat assessment. IEEE Transactions on Aerospace and Electronic Systems. 2008; 44(3):1060–9.
[7] Hess AOEB. Specification of adaptive security protocols-secure and trusted mediation layer for wireless sensor networks. Trustworthy Wireless Industrial Sensor (TWIS) Networks; 2013
[8] Potroneo D, Graziano A, Russo S. Security requirements in service oriented architectures for ubiquitous computing. Proceedings of the 2nd workshop on Middleware for pervasive and ad-hoc computing, ACM. 2004. p. 172–7.
[9] Da K, Dalmau M, Roose P. A survey of adaptation systems. International Journal on Internet and Distributed Computing Systems. 2011; 2(1):1–18.
[10] Evesti A, Suomalainen J, Ovaska E. Architecture and knowledge-driven self-adaptive security in smart space. Computers. 2013; 2(1):34–66.
[11] Mayrhofer R, Schmidtke HR, Sigg S. Security and trust in context-aware applications. Personal and Ubiquitous Computing. 2014; 18(1):115–16.
[12] Li F, Pienkowski D, Van Moorsel A, Smith C. A holistic framework for trust in online transactions. International Journal of Management Reviews. 2012; 14(1):85–103.
[13] Yan Z, Zhang P, Vasilakos AV. A security and trust framework for virtualized networks and software-defined networking. Security and Communication Networks; 2015.
[14] Wilson C, Hargreaves T, Hauxwell-Baldwin R. Smart homes and their users: a systematic analysis and key challenges. Personal and Ubiquitous Computing. 2015; 19(2):463–76.
[15] Alia M, Lacoste M. A QoS and security adaptation model for autonomic pervasive systems. 32nd Annual IEEE International conference on Computer Software and Applications, COMPSAC’08, IEEE; 2008. p. 943–8.
[16] Thomas RK, Sandhu R. Models, protocols, and architectures for secure pervasive computing: Challenges and research directions, PerCom Workshops; 2004.
[17] Fahrmair M, Sitou W, Spanfelner B. Security and privacy rights management for mobile and ubiquitous computing. Workshop on UbiComp Privacy; 2005. p. 40.
[18] Cappiello C, Comuzzi M, Mussi E, Pernici B. Context management for adaptive information systems. Electronic Notes in Theoretical Computer Science. 2006; 146(1):69–84. Han DM, Lim JH.
[19] Han DM, Lim JH. Design and implementation of smart home energy management systems based on zigbee. Transactions on Consumer Electronics. 2010; 56(3): 1417–25.
[20] M. Caruso, C. Di Ciccio, E. Iacomussi, E. Kaldeli, A. Lazovik, and M. Mecella, “Service ecologies for home/building automation,” in *Proc. 10th International IFAC Symposium on Robot Control (SYROCO 2012)*, 2012.
[21] M. Vega-Barbas, D. Casado-Mansilla, M. Valero, D. Lópezde- Ipina, J. Bravo, F. Flórez, and others, “Smart spaces and smart objects interoperability architecture (S3OiA),” in *Innovative Mobile and Internet Services in UbiquitousComputing (IMIS), 2012 Sixth International Conference on*, 2012, pp. 725–730
[22] M. J. Santofimia, X. del Toro, F. J. Villanueva, J. Barba, F.Moya, and J. C. Lopez, “A Rule-Based Approach to Automatic Service Composition,” *Int. J. Ambient Comput.Intell.*, vol. 4, no. 1, pp. 16–28, 2012.

[23] F. J. Villanueva, D. Villa, M. J. Santofimia, F. Moya, and J.C. López, "A framework for advanced home service design and Management," *Consum. Electron. IEEE Trans.*, vol. 55,no. 3, pp. 1246–1253, 2009
[24] J. M. Reyes Alamo, "A Framework for Safe Composition of Heterogeneous Soa Services in a Pervasive Computing Environment with Resource Constraints," Iowa State University, Ames, IA, USA, 2010.
[25] M. Faure, "Management of Scenarized User-centric Service Compositions for Collaborative Pervasive Environments.," Universit{é} Montpellier II-Sciences et Techniques duLanguedoc, 2012.
[26] A. K. Dey and G. D. Abowd, "Towards a Better Understanding of Context and Context-Awareness,"*Comput. Syst.*, vol. 40, no. 3, pp. 304–307, 1999.
[27] J. P. Sousa, V. Poladian, D. Garlan, B. Schmerl, and M.Shaw, "Task-based adaptation for ubiquitous computing," *IEEE Trans. Syst. Man, Cybern. Part C Appl. Rev.*, vol. 36,no. 3, pp. 328–340, 2006.
[28] J. P. Sousa, B. Schmerl, P. Steenkiste, and D. Garlan, "Activity-oriented computing," *Adv. Ubiquitous Comput.Futur. Paradig. Dir.*, pp. 280–315, 2008.
[29] A. Messer, A. Kunjithapatham, M. Sheshagiri, H. Song, P.Kumar, P. Nguyen, and K. H. Yi, "InterPlay: a middleware for seamless device integration and task orchestration in a networked home," in *Fourth Annual IEEE International Conference on Pervasive omputing and Communication*
[30] Oh S, Sandhu R. A model for role administration using organization structure. Proceedings of the 7th ACM symposium on Access control models and technologies, ACM. 2002; p. 155–62.
[31] Diep NN, Hung LX, Zhung Y, Lee S, Lee YK, Lee H. Enforcing access control using risk assessment. 4th European Conference on Universal Multiservice Networks, IEEE; 2007. p. 419–24
[32] Fadhel AB, Bianculli D, Briand L. A comprehensive modeling framework for role-based access control policies. Journal of Systems and Software. 2015.
[33] Choi D, Kim D, Park S. A framework for context sensitive risk-based access control in medical information systems. Computational and Mathematical Methods in Medicine. 2015.
[34] Bahtiyar S, Caglayan MU. Trust assessment of security for e-health systems. Electronic Commerce Research and Applications. 2014; 13(3):164–77.
[35] Jovanovikj V, Gabrijelcic D, Klobucar T. A conceptual model of security context. International Journal of Information Security. 2014; 13(6):571–81.
[36] Mowa Y, Abou-Tair D, Aqarbeh T, Abilov M, Dmitriyev V, Gomez JM. A context-aware adaptive security framework for mobile applications. Proceedings of the 3rd International Conference on Context-Aware Systems and Applications, ICST -Institute for Computer Sciences, Social Informatics and Telecommunications Engineering; 2014. p. 147–53.
[37] Charles PJ, Kumar S. Design of a secure architecture for context-aware web services using access control mechanism. International Conference on Contemporary Computing and Informatics, IEEE; 2014. p. 780–4.
[38] Kalidindi RR, Raju KVSVN, Kumari VV, Reddy CS. Trust based participant driven privacy control in participatory sensing. International Journal of Adhoc, Sensor and Ubiquitous Computing. 2011; 2(1).
[39] Sahil SB, Arnab R, Kanti NM. Trust evaluation based on nodes characteristics and neighbouring nodes recommendations for WSN. Wireless Sensor Network. Scientific Research Publishing; 2014.
[40] Agrawal CS, Khapre RR, Dhamande CS. A survey paper on the network security for application. International Journal for Reseach in Emerging Science and Technology. 2015; 2(1).
[41] Petraki E, Abbass H. On trust and influence: A computational red teaming game theoretic perspective. Seventh IEEE Symposium on Computational Intelligence for Security and Defense Applications. IEEE; 2014. p. 1–7.
[42] Yeun CY. Security for emerging ubiquitous networks. Journal of Networks. 2005; 1:2.
[43] Iltaf N, Ghafoor A, Hussain M. Step-: An algorithmic approach towards trust based security in pervasive computing environment. Proceedings of Asia-Pacific Services Computing Conference (APSCC). IEEE; 2011. p. 330–6.
[44] Basu J, Callaghan V. Towards a trust based approach to security and user confidence in pervasive computing systems. IEEE International Workshop on Intelligent Environments; 2005.
[45] Hammer S, Winer M, Andre E. Trust-based decision-making for smart and adaptive environments. User Modeling and User-Adapted Interaction; 2015. p. 1–27.
[46] Kagal L, Finin T, Joshi A. Trust-based security in pervasive computing environments. Computer. 2001; 34(12):154–7.
[47] Evans JB, Wang W, Ewy BJ. Wireless networking security: open issues in trust, management, interoperation and measurement. International Journal of Security and Networks. 2006; 1(1–2):84–94.
[48] Boukerch A, Xu L, El-Khatib K. Trust-based security for wireless adhoc and sensor networks. Computer Communications. 2007; 30(11):2413–27.
[49] Yan Z, Prehofer C. Autonomic trust management for a component-based software system. IEEE Transactions on Dependable and Secure Computing. 2011; 8(6):810–23.
[50] Yaich R, Boissier O, Jaillon P, Picard G. An adaptive and socially-compliant trust management system for virtual communities. Proceedings of the 27th Annual ACM Symposium on Applied Computing, ACM. 2012. p. 2022–8.
[51] Djordjevic I, Nair SK, Dimitrakos T. Virtualised trusted computing platform for adaptive security enforcement of web services interactions. IEEE International Conference on Web Services; 2007. p. 615–22.