Indian Journal of Science and Technology, *Vol 9(48), DOI: 10.17485/ijst/2016/v9i48/89396, December 2016*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Adaptive Security Schemes based on Context and Trust for Ubiquitous Computing Environment: A Comprehensive Survey

G. Jagadamba[1]* and B. Sathish Babu[2]

[1]Department of ISE, Siddaganga Institute of Technology, Tumakuru - 532103, Karnataka, India; jagadambasu@gmail.com
[2]Department of CSE, Siddaganga Institute of Technology, Tumakuru - 532103, Karnataka, India; bsb@sit.ac.in

Abstract

Objectives: To present the principle of working of some of the widely used adaptive security schemes in the domain of ubiquitous computing. **Methods/Statistical Analysis**: The main focus of the study includes analysis of the security schemes with respect to the use of security parameters such as context and trust. Many security schemes applied for various applications are considered and evaluated by considering the security credentials such as access control, privacy, and context-awareness. The study finds context and trust as essential to develop adaptive and accurate security framework. **Findings:** The paper identified different taxonomies built for trust, context, policy and adaptive security. It pointed many solutions to couple with the security issues like access control, and authentication that are more appropriate to the today's world. It also discussed many security and implementation credentials with a review summary and suggested the findings could be used to propose adaptive security frameworks which can offer the required level of security. **Application/ Improvements:** The proposed framework can be used to applications built in the Ubiquitous Computing Environment (UCE) such as Ubiquitous-healthcare, U-learning, U-smart campus, and so on.

Keywords: Access Control, Adaptive Security, Context, Privacy, Trust, Ubiquitous Computing Environment

1. Introduction

A computing history[1] started with the centralized computing and followed with Client-Server computing, Internet computing, and Pervasive/Ubiquitous computing. Ubiquitous computing applications are found to operate in an open, dynamic, and flexible environment and have enough freedom in selection and utilization of services at any time and place. The high spontaneity and heterogeneity of ubiquitous computing environments include self-adaptive applications[2] that are essential to realizing the ubiquitous computing vision of invisibility and ubiquity. This nature of ubiquity and mobility require adaptive security issues including privacy, authentication, authorization, and trust. Usually, researchers concentrate on particular security aspects such as secure service discovery, context-aware services, or trust model, or risk aware security, intrusion detection without looking at the dynamic nature of the security requirements reflecting towards changing characteristics and requirements of the service requesters. There are no such works found which is aware of the deserved security level to the service requester's situation.

*Author for correspondence

In this regard, nowadays the computing environments include smart devices that are aware of the context in which they operate and adapt themselves to the new surroundings and requirements at the design time. A protection scheme defined at the design time is not enough and cannot be considered to provide the security in the operational environment. However, protection schemes deployed automatically at run-time conquers much security issues to the current safety requirements of the environment[3]. The adopted security should continue to protect service access from unauthorized or malicious entities, even when security concerns change dynamically[4]. To do so many technologies are proposed, but most of them were found to be static in nature. Hence, the primary concern of this study is to identify the attributes to design an adaptive security scheme which will work dynamically by adopting the changes happening in the heterogenic computing world.

1.1 Requirements for Adaptive Security

Adaptive security is an aggregation of security measure with continuous monitoring to detect or prevent vulnerabilities/risk and act for the new assessed threats[5] based on the capacity of the node. The security adaptation is not a new concept[6]; it is the desirability of a system that adapts security in an autonomous manner, to answer as quickly and efficiently to perceived threats in its environment. In conjunction with the above, an adaptive security is defined as the "security solution/protocol that senses, learns the changes in the environment, device capacity, variations in the network services with the anticipated threats and to adopt the new security requirements and execute itself without the intrusion of the humans".

To achieve the required security in ubiquitous computing and related technologies, it is necessary to have adaptive mechanisms/policies[7]. At the same time, the security mechanism should be aware of the context of the device for computation while performing the analysis of the user behaviour or environment. Thus, there is a need to focus the research on the adaptive security by considering the vulnerability of the operating context. From[8,9] adaptations does not only mean dynamic loading/replacement of software components or technologies but satisfying the requirements of an application adaptation.

In the context-aware systems, the untrusted users also pose the security problems. Hence, the security credentials necessarily give scope to[10] the user trust and security in context-aware systems with the feature of adaptability. The exposed real world applications such as military applications, health care management, tourism, e-business[11] smart spaces[12,13] like - home, offices, university, etc., require adaptive security approaches while providing the services.

Many research works stressed the importance of context and trust in the resource constrained ubiquitous computing environment. The changing computing resources, accessing services, network, contexts, and user trust characterized the ubiquitous environments a need for context-aware self-adaptive systems[14]. According to[15], the ubiquitous/pervasive computing includes a complex socio-technical system that needs beyond traditional system-centric approaches for designing security with a well-approached analysis. Hence, we concentrate more on designing the framework based on contextual and trust analysis to define the adaptive security[16,17] level based on the requirement in the ubiquitous environment.

In our survey the security schemes are placed under the following two categories:

- Context based security
- Trust based security

In second, third and fourth section discusses the security schemes based on context, trust and adaptive security issues reviewed with the design and relevant security issues. In the last section, we attempted to summarize the schemes with the various research works done under context, trust and privacy issues.

2. Context-based Security

This section discusses the definition of context, applicability, role and adaptability of the context attribute to design security framework. The concept of context has started from 1990 when Mark Weiser introduced the term ubiquitous computing. The context-awareness focused towards the desktop to mobile device, physical sensors to virtual sensors and vehicular devices to body wear devices. Many definitions are defined by many researchers, but found to be application specific or nearly to the operational environment based. We define the context in the ubiquitous environment as

"Context as any information that is utilized to identify, analyse, and describe the requirements and the situation of an entity, which can be used to support the required services or applications".

The greater challenges are faced while developing frameworks to address security and privacy issues in the context-aware systems[18]. The context-aware services raise

a risk of security and privacy, but a distinct approach keeps these risks behind. On the contradictory, context awareness enhances the effectiveness of the mechanisms by incorporating contextual data into a decision-making process[19]. Thus, the usage of context[20] to provide security was considered as a primary attribute of the ubiquitous network, where the services more often are context-aware.

From the works[16–19] done under context-aware environment, the taxonomy of the context for security in the ubiquitous computing environment is proposed in Figure 1. According to our view, the context can be behavioural, computing or physical. The physical contexts talk about the user and environmental context like temperature, light, noise, location, etc. The computational context considers the computational task like capacity, communication overhead, and associated processing overhead. The behavioural context is about location, time, situation, risk management, and activity about to adaptive or non-adaptive nature. Utilizing the context, a new approach called, "context-based security" was proposed[21] through context policies. The new security policies can be set to identify the enforced mechanism for the new scenario. Thus, the security policies based on context gets on appropriate mechanism to enforce the required level of security for the existing or future situations. In the following subsections, we discuss some of the categorization that suited in the context-aware security approaches in the ubiquitous computing environment.

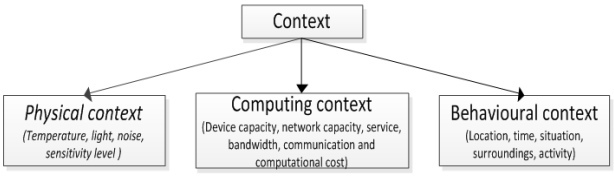

Figure 1. Taxonomy of context.

2.1 Adaptive Nature in Context based Security

The idea of adaptive and ubiquitous systems is already a subject of intense research for several years to realize context information as intellectual property while enforcing the security[16]. The technologies evolved nowadays enable users to access services using multiple channels. Though most of the channels assure secure communication, it is not remarkable practically. Hence, a well-managed context-aware security characterization to service access by adaptivity and multichannel access is much concentrated[17]. The adaptation includes context lifecycle approach and we defined our own context life cycle in Figure 2 with the peer review[16,17].

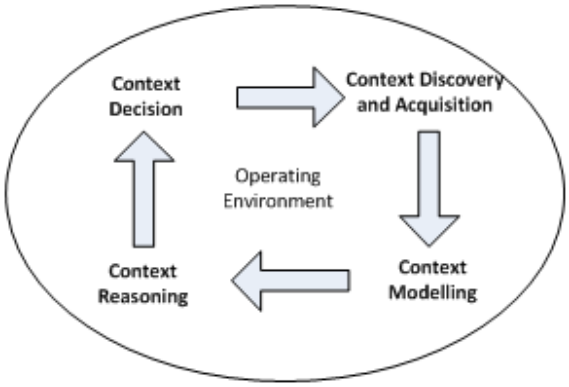

Figure 2. Context life cycle.

Context discovery and acquisition includes discovery of the new context in the operating environment and then to acquire for modelling. The acquisition techniques include pull and push technique, through sensors, and sources. The procedures of acquisition vary from application to application, but the acquisition data remains the same. The context modelling be based on the static polices or adaptive policies. Preferably for heterogeneous environment, adaptive context modelling techniques are most solicited and are our topic of concern. The context reasoning evaluates the outcome of the modelling done based on ontology[6], graphical[12], object based, mark-up language schemes, etc. These reasoning are helpful for context decision. The context decisions are in the final stage of lifecycle that intimates the entity to adapt accurate decision.

While doing context acquisition, modelling, and reasoning, a care is needed to provide security and privacy. A well-defined security protocols protect and save the context. Several research works concentrate on providing the security and privacy for context-aware applications based on policy, contents, profiles, rules, etc., but the context decision in context-aware security applications need to understand the requirements and demands of the situation without the intrusion of the human to organise and structure the dynamic operability of its internal components.

Many works lag to include adaptivity, hence the consideration of context life cycle while designing may experience adaptivity. In the below works we review the adaptive

security protocols that adopted context as a main parameter. In[12] appropriate security levels for a pervasive application was presented through the contextual graphs by making the security decisions as action with the user's role, time of operation, the domain of request arrived. The consideration of the incremental acquisition of new context made the proposal nonadaptive towards security and raised the risk in the environment. In this situation, a risk management for the new context information representing changes in the environment and usage of an application was found as a new solution[22–26]. Towards this, a flexible and autonomous adaptation in resource restricted mobile devices used in smart spaces based on ontology was proposed. The start-up and run-time phase adaptation were used for data assets by the risk-based security measurements in different threat situations. But, the theoretical approach works in the same communication domain.

An assessment framework[27] evaluates the context-aware adaptive security based on processing capability and resources available for the Internet of Things (IoT) in e-Health application. Many organisations like Cluster of European Research Projects on the IoT (CERP-IoT)[28] focused their time bound research and development on context-aware computing on the IoT during 2015-2020. The framework addressed the specific requirements related to the context, the data communication, the devices, and the actions of the involved actors in the health care system. The measurable data from sensors were used as training data towards adaptive security. The framework applies to any quality of service requirements but fails towards situation based security for the applications and changing conditions in the operating environment. In compliment with the situation based security a Role-Based Access Control (RBAC) composed for the user, role, session, User-Role Assignment (URA), Permission-Role Assignment (PRA), role hierarchy, and constraints was found[29]. But, RBAC fails to fulfil the need of adaptive security[30] in a new environment like ubiquitous environment. Hence, a Model-Driven Engineering (MDE) approach, UML and the Object Constraint Language (OCL) is proposed to enable the precise specification and verification of the classified RBAC policies[31]. Here, the policies are selected for analysis and classification of the various RBAC. Due to the non-dynamic nature of temporal and spatial contexts, the proposal was categorized into the nonadaptive model. Still now we are able to clearly analyse that, the context can play a role either in defining the attributes for security or policy creation. In the next few works, we review some more context related works about the user and environment behaviours.

A framework based on context-aware access control proposed[32] a model based on a need-to-know principle. It considered the access control by evaluating the risk of the users request in the corresponding context and grants permission only when the request falls below an acceptable level of risk. The framework traced the requirements of the user to establish a treatment-based permission profile by accumulating and analysing the data access history. The access control was allowed by policy and predefined context (critical, dangerous, and stable) management. This was one of the schemes which adopted the dynamic policies, but contextual definitions were found to be static. To make the context policies dynamic, the recommendation from trusted professional[33] is required. Here, the trust assessments metrics are utilized to a particular property access of a security system to make the model flexible in its approach and facilitates an entity trust depending on the contextual need. Finally, these work stressed the importance of trust in the context to adopt the dynamic security policies in the changing environment.

2.2 Communication and Energy Consumption Overhead in Context based Security

The object-oriented middleware facilitated the context-sensitive communication in ubiquitous computing[23]. The consumption of large amount of energy, non-interoperability among reconfigurable objects and non-adaptive operability for frequent context changes in real-time makes the proposal made to dawdle towards energy consumption overhead. A context sensitive communication for service discovery based on ontology for large scale ubiquitous network to support scalable semantic queries with low communication overhead was proposed[24]. Context-sensitive communication and information tools were developed and tested[25] for easier implementation, maintenance, to support different types of terminals, networks, and services, security and usability requirements. For the potential utilization of the mobile terminal, the security concerns and handling with the user interface requires accuracy with each application. Our previous work concentrated on energy efficient adaptive context-aware access control design for accessing the web in a centralized approach[26]. The nature of adaptivity was implemented based the activity done in the history, type of service requested, time, location and purpose. Contradictory[27] proposed context-aware access control architecture to secure

web service using environment roles played by the user. Both the work was an attempt to provide adaptability with minimum computation energy. The capturing of relevant security context of the environment with minimum energy will make the models more applicable in any computing environment. Hence, a context-aware adaptable, energy efficient model was in need to design the security framework.

2.3 Risk Management in Context based Security

A conceptual model, which is an area of modelling[34] identifies the security context and takes related social aspects into account through a set of appropriate superficial level of abstraction. Conceptual models[34] were not promising towards the security management to the new security policies and risk management. Other than authentication and authorization security issues, a risk of privacy issue is raised in the context-aware security schemes. In this regard, a privacy-preserving security challenges for a mobile user were addressed[35] in context-aware adaptive security framework through judging and adapting the context information by security control measures. Here, mobile applications are executed through incubators to control the communication between the application and the device resources worked through a standalone application. An Analytic Hierarchy Process (AHP) structured to evaluate the disclosure of user context (location, time, activity, etc.,) by providing the risk level and suggesting the appropriate security control decision. A similar approach to provide security, based on context was proposed[36] about the inclusion of trust attributes to minimize the risk of the access control decisions.

2.4 Summary

The context-based security initiated new security problems due to mobility and heterogeneity in ubiquitous and pervasive computing. The effective means of context acquisition mechanisms, context composition techniques and adding context to security decision can reduce the security related problems. But the security policy based on context should be able to work in the changing and resource constrained environment. At the same time, the context based security can overcome the risk management when trust attribute is included. Hence, a context based security for trusted entity is necessary for the current scenario. Finally, security policies based on adaptive context analysis for the risk aware environment are considered to develop an adaptive security scheme.

3. Trust based Security

In this section, we discuss the definitions, taxonomy and need of trust in designing the security scheme. The major review was concentrated on the design issues on energy efficient trust evaluation and adaptivity in developing the security framework.

The trust has influenced in many disciplines of computing networks. But, the negligence or absence of trust resulted in the delayed service access, communication, and business anticipation. Hence, trust is used as one of the security parameter while providing the service access in the ubiquitous networks. As trust is subjective, it is associated with the physical and digital context while evaluating. At the same time, the appropriate trust evaluation decisions in the ubiquitous network suppress or avoid the risk factors associated with the untrustworthy entities. Hence, a well-designed and appropriative trust evaluation model is necessary to overcome the security risk in the UCE.

Conceptually, trust is a parameter, used to exchange information regarding the entities actions through belief and faith. The belief or faith advances through a series of interactions done over time. Interactions may be direct or indirect. In the ubiquitous environment, positive behaviours increase the trust, and negative behaviours decrease the trust upon the entity. Many researchers classified the trust into proofs and indicators[37,38]. The proofs are certified information (identity, property and authorization) issued by the certification authority or from other central controlled systems. While indicators are possible factors stored internally or externally collected from various sources[39]. In trust evaluation, the indicators are valuable hints when certification authority does not exist. Indicators are subdivided into reputations, experience and recommendations concerning to the operating ubiquitous environmental context[40]. Hence, researchers concentrated to include trust while developing the security schemes.

Many researchers have mentioned that the availability of trustworthy nodes, solve the security challenges in the network[41]. Hence, trust based security is required rather than regular authentication and access control. By adding greater flexibility in designing policies, trust provides more control over accessing services and information. Thus, the involvement of trust evaluation and management in providing security about the context-aware embedded in the security system[42]. Hence, trust is considered as a new research attributes[43] in the field of adaptive security. The evaluated trust levels are utilized for decision-making[44] in smart environments. Moreover, trust is not defined once and continued

forever, but developed according to the need and more often changes by time in the ubiquitous environment. Hence, a computational intelligence for trust pointed the influence and transfer of trust as interdisciplinary research work[45]. By considering the trust definition, taxonomy of trust for the security is proposed in Figure 3. The taxonomy is based on the requirements of trust on services, the context of the operation, attributes for the evaluation of the entity or service, policy for the operating environment and entity role-based trust. By keeping the taxonomy classifications some of the works in the field of trust evaluation and operation in providing the security framework is discussed.

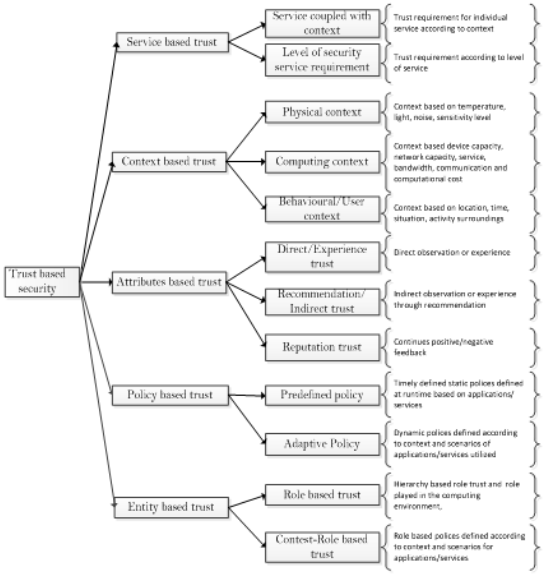

Figure 3. Taxonomy of trust.

3.1 Trust Evaluation and Policy based Trust Security

The integration of trust[46] extended the security infrastructure by designing the policies and control over accessing services/information. The usage of ontology based policies is assigned dynamically or created to the new role by introducing the trust factor. These frameworks can handle only when the trusted party knows the users in the same operating environment. But, the environment is not able to present some of the factors such as:

- how trust is evaluated
- how much trust is required and
- how much access control is possible.

The absence of this evidence was the drawbacks of the proposal in the last decades. The drawbacks are extended to the implementation and efficiency factors also. To overcome the drawbacks of trust evaluation and implementation, an efficient adaptive policy and trust management[47] was proposed. The trust management works also handled the malicious strategic behaviour by calculating direct trust. The models combined the ability to reason human cognitive behaviour and capability to adjust the change in behavioural pattern. The works concentrated more on trust evaluation than implementation and identification of available resources for trust computation. These things decreased the user confidence while accessing the services in the web. To increase the user confidence, a trust-based architecture[48] with the role-based access control system was developed. Then the architecture will be an extended version of the generalized role based access control system to make the security policies more flexible. The object-centric policies are better in these cases compared to subject-centric policies. Hence, the access request to any resources is based on subject credentials and identity or location context. These models ensure the privacy for the higher computational and processing devices. Hence, the new generations require less object-centric trust evaluation and utilization of trust in designing the new security policies for access control.

3.2 Energy Efficient Trust Security

The trust evaluation consumes a lot of energy as; it is not evaluated once and used forever. Hence, any model of its kind consumes more energy when it comes to adaptive trust evaluation for security design. In this regard, some of the schemes were reviewed and found some interesting factors to be adopted about the trust assessment and utilization while developing the security framework.

A model generating the trust autonomously by categorization of trust level is proposed[49] to reduce the computational processing time. But it requires a centralized and manual administration to reduce the computations. Hence, utilization of fuzzy numeric values is assumed while computation, communication, and storage by extracting the context of the mobile users. To operate in different domains a large amount of storage and the computational memory became a major problem. A concept of clustered networks as a backbone and a mobile agent system to achieve minimal overhead regarding additional messages was attempted[49]. The assumption of trusted authority responsible for generating and launching mobile agents made the works more resilient against the unauthorized analysis and modification of computation

logic. Hence, a concept of maintaining a localized trust and reputation management strategy was attempted to avoid network-wide flooding in the wireless network. But the restriction of the deployment in the large scale ubiquitous network was the major drawback to consider these design issues. These drawbacks motivated us to find new techniques/algorithms towards the implementation of security using trust in a large scale ubiquitous network with minimum process time and memory computation.

In this regard, works in large-scale were studied and found some interesting things about the trust. Many works stressed the significant role of trust in e-business in the world of online shopping. Where reputation plays a prominent role when we are talking about context based trusted transaction[50]. To secure e-business transaction an access control through adaptive trust negotiation and access control was proposed[51]. By doing so, an effort to overcome the "phishing" attack has been included by continuous trust evaluation and updating the same for security levels definitions. But, the absence of the adaptability and efficiency resulted in new attacks making the security approach very week in the ubiquitous network[11]. The User Trust Model (UTM)[44] or automatic decision making for smart and proactive environments was based on Bayesian networks. The model was energy efficient by making use of the user's actions at present by neglecting the past behaviours. But, the centralized approach with single user preference modelling made it feebler to work in the UCE. Inconsistent to these, we moved towards adaptive trust models which are energy-efficient to design adaptive security framework.

3.3 Adaptivity in Trust Security

A new concept of adaptive trust framework was developed[52] to provide security in resource constrained environment by keeping the capacity and service offered in the ubiquitous network. The adaptive trust includes the selection of trust attributes (direct, indirect, context, prejudice and social) according to the type of service requested and on the available resources in the device. The work was adaptive towards the trust attribute selection for security but failed to incorporate trust evaluation. Most of the adaptive trust models concentrate on energy efficient models rather than identifying the unauthorised entities. In this sense, a lightweight trust based authentication protocol[53] had a potential to protect the entities from the malicious attacks by incorporating the trust model into tiny mobile devices with limited resources and bandwidth.

A full pledged adaptive security protocol[12] was designed for trust evaluation and security for large/small scale or open/dynamic ubiquitous computing environment. To enhance security, an adaptive trust management protocol for Internet of Things (IoT) was considered[54] by evaluating the trust using direct communication and the recommendation as a decentralized trusted authority for a user-centric social IoT environment. The analysis of the two real-world social IoT applications was mentioned, and the results were promising. By imparting the complicated mechanism and adaptivity has been achieved to some extent. A method of multilevel trust models[55] were in progress by utilizing the trust factors/attributes like experience, recommendation, and knowledge for computing the trust level of the entity based on the application context. But, the complexity of trust level increases the system computation cost and overhead with the security level and application type.

A mutual trust[56] stresses more on authentication, access rights, and privileges to the retrieved information in the ubiquitous computing environment. The concept of mutual trust not only provides access control but also helps in service discovery and sharing[57]. It emphasizes on the change of trust value and security level depending on the service, the service provider, and the service requester. A trust-based service management for each node participating as the service provider or a service requester in service-oriented MANETs (Mobile AdHoc Networks) was proposed[54] for effective trust management. Thus, efficient trust management became an alternative solution when compared to distrusted or single-trust-based solutions. Finally, the works pointed towards energy efficient trust computation and utilization in the changing environment.

3.4 Summary of Trust based Security

The review was able to provide insight towards various aspects of trust computation while designing the adaptive security based on trust. We listed some of the following findings while developing the adaptive security:

- Proper trust computation/evaluation through relevant trust attributes, preferably (Direct trust, Recommendation Trust, Social Trust, Prejudice Trust, Context Trust)
- Categorization of trust levels according to the security requirement.
- Methodologies to overcome phishing and malicious entity attacks while trust computation.

- Adaptive nature with energy efficiency in the resource constrained and dynamically changing environment.

At the outcome, a trust-based security designed with a suitable trust evaluation model in the decentralized ubiquitous computing environment was the first choice. Then computation and utilization of trust are considered based on the available capacity and service is a context-aware approach towards security.

4. Review Summary of the Adaptive Security in Context and Trust based Security Paradigm

Adaptive security solutions are designed to ensure a high level of authentication, fine-grained mechanisms for authorization, sensibility to external and internal limitations to security (e.g., capacity of the computing resource, speed, algorithms) and ability to deal with abnormal conditions (e.g., need for special treatments to emergencies). The adaptive characteristics[55–58] include -response time, effectiveness, flexibility, robustness and self-defective model to reflect the changes in real time applications.

The inclusion of context and trust will make the new adaptive security framework more reliable to the today changing and heterogeneous environment. By considering these factors, we propose taxonomy in Figure 4 that represents the security attributes towards adaptive characteristics. The adaptivity can be achieved either using contextual information's or through trust factor. But, the combination of context and trust will make the security framework more adaptive and efficient.

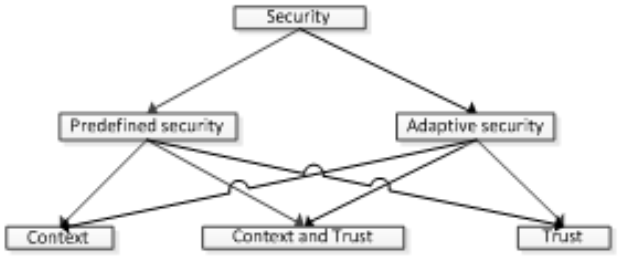

Figure 4. Taxonomy of security in ubiquitous computing environment.

Concurrently, we summarized the research works review based on context and trust parameters used to provide security. The evaluations of the works are based on the methodologies and techniques with the adaptability and application. The method was based on object or policies or ontology etc. The modelling based on the creation of testbed, simulation, real-time implementation or experimentation set up or application design.

In Table 1 summarized all the factors with the performance and application use of the research work in the last column. In Table 2 provides the review summary of security analysis based on the access control operation implementing both authentication and authorization. The association of trust and context aggregation or association is to design a security model and our concern about security schemes was based on changing scenarios and adaptive nature to tackle all the changes happening in the environment while preserving the privacy of the user. Hence, last two columns of the dealt with the privacy preservation factor and the approach to provide adaptive security. Some of the notations are used to verify the review factors in the Table 1 and Table 2. In this regard, the access control, trust, context, and privacy are represented with the notion of YES- for inclusion, NO- for not considering the security attributes and P-for partial. The adaptive factor is represented as - A, non-adaptive as - NA, partially adaptive as-PA and not applicable as-NA is considered as notations for the adaptive security paradigm approaches. To accomplish the survey, the security issues[28,23,25,59–61] were strongly considered as the context-related and context-independent features. Keeping in mind the research work[2,26,62,63] are adaptive for the dynamic changes in the adaptation of working either to internal or external context. The works[40,49,50] strongly recommend the usage of trust in access control for services or resources in the network. But, the significance of context and trust is stressed[9,46] to provide security. On the contradictory most of the works are found to be non-adaptive[23,24,27,33,48] or partially adaptive[9,14,21,22,25,28,39,42,49,50,64,65] to provide security in the ubiquitous computing network.

Finally, we strongly intend to design the adaptive security framework based on the following adaptations suitable for the heterogeneous network such as the ubiquitous, pervasive and mobile networks.

- Incorporation of self-adaptive nature in the operating and computing environment.
- Adaptive service access methodology based on the context and trust attributes.
- A proper continuous monitoring, classification, analysing is required to greater the new applicable security policy planning and execution of the same for services, applications and devices are required.

Table 1. Contribution of research work to security

REF.	METHODOLOGY	MODEL	APPLICATION
21	Contextual graphs as a modeling tool for managing security polices	Mathematical model	Case study about the access control of health care records of hospital.
22	Ontology based adaptive security	Case study modeling	Smart space environment
23	Object based	Testbed middleware model	Real time application level implementation.
24	Ontology based semantic mapping for service discovery	Context based service discovery	Simulation
25	Context content based	Service based architecture	Testing environment for health monitoring
26	Dynamic context analysis	Context based self-adaptive	Application level
64	Dynamic policy based	Analytical	----------
28	Algorithm based	Experimental and simulation evaluation methodology	e-Health application with assessment of human observers.
35	Analytic hierarchy process (AHP) structured technique	Context based model	Prototype application on Android OS
39	Trust based key generation and distribution	Security protocol model	Application level
46	Ontology based access control for services	Trust based architecture	Proposed for smart offices
48	Static policy and trust based	Intelligent application environment	Application level
14	Adaptive context	Self-adaptive model	Application level
51	Policy and trust based	Real-time application model& e-business application level	E-business application level implementation.
2	Ontology-based context modeling methodology based on self-adaptation policies on utility functions	Service-based application model based on formal semantics and XML-based language	Human tracking application for the user presence in home, way to gym and at gym.
53	Trust model	Simulation model	Service provision application for Android phones.
9	Adaptation loop, Information Security Measuring Ontology(ISMO) and a smart space security-control model	Generic conceptual level	Specific to smart spaces like home and offices.
33	Entity oriented modeling for trust assessment	Simulation model	Health care application compared with Cell Peer and Fire trust models.
54	User-centric system model	Table-lookup analysis methodology (sensitivity and cost)	Web applications
32	Role-based and risk-aware	Specific model	Medical Information System.
31	Precise specification and verification of RBAC policies	A conceptual and model-driven	A situational-aware application for treating refuges and causalities in emergency scenarios.
44	Bayesian Network based &Specific model	Specific model	Smart office designed for user trust
58	Multi trust based algorithm	Estimation of trust value	Service oriented MANET application
62	Context attribute based	Estimation of user behaviour	Service oriented adaptive control over small scale ubiquitous environment

Table 2. Contribution of research work with respect to security attributes

	ACCESS CONTROL	TRUST	CONTEXT	PRIVACY	ADAPTIVE SECURITY
[28]	NO	NO	YES	P	PA
[21]	YES	NO	YES	NO	PA
[22]	YES	NO	YES	NO	PA
[23]	YES	NO	YES	NO	NA
[24]	NO	NO	YES	NO	NA
[25]	YES	NO	YES	NO	PA
[26]	YES	NO	YES	P	A
[64]	YES	NO	YES	NO	NA
[35]	NO	NO	YES	YES	PA
[39]	YES	YES	NO	NO	PA
[46]	YES	YES	YES	NO	PA
[48]	YES	YES	NO	NO	NA
[51]	YES	YES	NO	NO	PA
[14]	NO	NO	YES	NO	PA
[2]	NO	NO	YES	NO	A
[53]	YES	YES	NO	NO	PA
[9]	YES	YES	YES	NO	PA
[33]	YES	YES	NO	NO	NA
[58]	NO	YES	P	NO	PA
[32]	YES	NO	YES	NO	PA
[31]	YES	NO	YES	NO	PA
[44]	YES	YES	NO	NO	PA
[58]	YES	YES	NO	NO	PA
[62]	YES	NO	YES	P	A

- By considering the above design issue, an adaptive security scheme will make the communication network more secured.
- Privacy preservations[65] while making adaptive security scheme is needed (the context acquisition is done to make the system adaptive to the new changes).

5. Conclusion

Security and trust have been a challenge for ubiquitous computing from the beginning. The context provides the meaningful understand of the situation or data but increases the security threats due to possible misuse of identity, location, activity, and behaviour. Even though security issues are addressed at the context-aware applications level, it is merely not attended in the context-aware middleware level. Therefore, security protection requirements need to be carefully addressed by the incorporation of trust. The evaluation of trust and utilisation of trust in context-aware applications are in of important issues.

This study pointed many solutions to couple with security issues. The solutions that are more appropriate to the today's world have been discussed here with many security and implementation credentials. On the overall, the adaptability provides an independent platform towards many security characteristics like authentication[66], authorization and access control associated with various heterogeneity parameters to ensure the security in the ubiquitous network. In conclusion, security based on trust and context placed a strong base for adaptive

security. The prioritising the adaptive trust attributes with the contextual information develops an adaptive security framework that can act accordingly to the dynamically changing environment.

6. References

1. 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.
2. 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.
3. 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.
4. 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.
5. 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.
6. Hess AOEB. Specification of adaptive security protocols-secure and trusted mediation layer for wireless sensor networks. Trustworthy Wireless Industrial Sensor (TWIS) Networks; 2013.
7. Cotroneo 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.
8. Da K, Dalmau M, Roose P. A survey of adaptation systems. International Journal on Internet and Distributed Computing Systems. 2011; 2(1):1–18.
9. Evesti A, Suomalainen J, Ovaska E. Architecture and knowledge-driven self-adaptive security in smart space. Computers. 2013; 2(1):34–66.
10. Mayrhofer R, Schmidtke HR, Sigg S. Security and trust in context-aware applications. Personal and Ubiquitous Computing. 2014; 18(1):115–16.
11. 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.
12. Yan Z, Zhang P, Vasilakos AV. A security and trust framework for virtualized networks and software-defined networking. Security and Communication Networks; 2015.
13. 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.
14. 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.
15. Thomas RK, Sandhu R. Models, protocols, and architectures for secure pervasive computing: Challenges and research directions, PerCom Workshops; 2004.
16. Fahrmair M, Sitou W, Spanfelner B. Security and privacy rights management for mobile and ubiquitous computing. Workshop on UbiComp Privacy; 2005. p. 40.
17. 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.
18. 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.
19. Habib K, Leister W. Context-aware authentication for the internet of things. Eleventh International Conference on Autonomic and Autonomous Systems [Internet]. [cited 2015 Dec 10]. Available from: Wolfgang Leister.
20. Dey AK. Understanding and using context. Personal and Ubiquitous Computing. 2001; 5(1):4–7.
21. Brezillon P, Mostefaoui GK. Context-based security policies: A new modeling approach. Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops, IEEE; 2004. p.154–8.
22. Evesti A, Ovaska E. Ontology-based security adaptation at run-time. 4th IEEE International Conference on Self-Adaptive and Self-Organizing Systems (SASO), IEEE; 2010. p. 204–12.
23. Yau SS, Karim F. An adaptive middleware for context-sensitive communications for real-time applications in ubiquitous computing environments. Real-Time Systems. 2004; 26(1):29–61.
24. Kang S, Kim D, Lee Y, Hyun SJ, Lee D, Lee B. A semantic service discovery network for large-scale ubiquitous computing environments. ETRI Journal. 2007; 29(5):545–58.
25. Mirkovic J, Bryhni H, Ruland CM. A framework for the development of ubiquitous patient support systems. 6th International Conference on Pervasive Computing Technologies for Healthcare (PervasiveHealth), IEEE; 2012. p. 81–8.
26. Jagadamba G, Babu BS. A dynamic Context-based Access Control (CAAC) system. International Conference on Emerging Computing and Information Technology, Elsevier: India; 2013.

27. Leister W, Poslad S, Hamdi M, Abie H, Torjusen A. An evaluation framework for adaptive security for the IoT in e-Health. International Journal on Advances in Security. 2014; 7.
28. Guillemin P, Friess P. Internet of things strategic research roadmap. The Cluster of European Research Projects, Technical Report [Internet]. 2009. Available from: http://www.internet-of-things-research.eu/pdf/IoT Cluster Strategic Research Agenda.
29. 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.
30. 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.
31. Fadhel AB, Bianculli D, Briand L. A comprehensive modeling framework for role-based access control policies. Journal of Systems and Software. 2015.
32. 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.
33. Bahtiyar S, Caglayan MU. Trust assessment of security for e-health systems. Electronic Commerce Research and Applications. 2014; 13(3):164–77.
34. Jovanovikj V, Gabrijelcic D, Klobucar T. A conceptual model of security context. International Journal of Information Security. 2014; 13(6):571–81.
35. 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.
36. 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.
37. 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).
38. 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.
39. 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).
40. 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.
41. Yeun CY. Security for emerging ubiquitous networks. Journal of Networks. 2005; 1:2.
42. 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.
43. 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.
44. 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.
45. Kagal L, Finin T, Joshi A. Trust-based security in pervasive computing environments. Computer. 2001; 34(12):154–7.
46. Almenarez F, Marn A, Campo C, Garcia C. PTM: A pervasive trust management model for dynamic open environments. First Workshop on Pervasive Security, Privacy and Trust. 2004; 4:1–8.
47. Zhang H, Wang Y, Zhang X, Lim EP. Reputationpro: The efficient approaches to contextual transaction trust computation in e-commerce environments. ACM Transactions on the Web (TWEB). 2015; 9(1).
48. Ryutov T, Zhou L, Neuman C, Leithead T, Seamons KE. Adaptive trust negotiation and access control. Proceedings of the tenth ACM symposium on Access control models and technologies, ACM; 2005. p. 139–46.
49. Aditya B, Babu BS. Capacity and service (CapServ) adaptive trust computation by territory formation in ubiquitous environment. Advanced Pervasive and Ubiquitous Computing. 2012; 4(4).
50. Rajesh AK, Mohan N. Multilevel trust architecture for mobile adhoc networks based on context-aware. Journal of Theoretical and Applied Information Technology. 2014; 59(2).
51. Djellali B, Chouara A, Belarbi K, Lorenz P. Design of authentication model preserving intimacy and trust in intelligent environments. Network Protocols and Algorithms. 2015; 7(1):64–83.
52. Chen R, Guo J, Bao F. Trust management for SOA-based IoT and its application to service composition. IEEE Transactions on Services Computing. 2015; 1:1.
53. El Husseini A, M'hamed A, El Hassan B, Mokhtari M. Trust-based authentication scheme with user rating for

low-resource devices in smart environments. Personal and ubiquitous computing. 2013; 17(5):1013–23.
54. Bhumika G, Zaveri MA, Rath HK. Trust based service discovery in mobile ad-hoc networks. Lecture Notes on Software Engineering. 2015; 3(4):308
55. 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.
56. Boukerch A, Xu L, El-Khatib K. Trust-based security for wireless adhoc and sensor networks. Computer Communications. 2007; 30(11):2413–27.
57. 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.
58. 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.
59. 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.
60. Wang Y, Chen R, Cho JH. Trust-based service management of mobile devices in ad hoc networks; 2015.
61. Rajarajeswari S, Somasundaram S. Data confidentiality and privacy in cloud computing. Indian Journal of Science and Technology. 2016 Jan; 9(4):1–8.
62. Jagadamba G, Sathish Babu B. Adaptive context-aware access control model for ubiquitous learning environment. International Journal of Information Technology Bharati Vidyapeeth's Institute of Computer Applications and Management (BVICAM). 2016; 8(1).
63. Perera C, Zaslavsky A, Christen P, Georgakopoulos D. Context aware computing for the internet of things: A survey. Communications Surveys and Tutorials. 2014; 16(1):414–54.
64. Jagadamba G, Sathish Babu B. Context and trust based adaptive security policy: A Survey. International Journal of Computer Systems. 2016; 3(2).
65. Nagaraju S, Parthiban L. SecAuthn: Provably secure multi-factor authentication for the cloud computing systems. Indian Journal of Science and Technology. 2016 Mar; 9(9):1–18.
66. Priya JK, Charles IP, Britto RS. Context-aware architecture for user access control. Context. 2014; 2(3).x