Context and Trust based adaptive security policy: A Survey

Jagadamba G\(^{A}\) and Sathish Babu B\(^{B}\)

\(^{A}\)Department of Information Science and Engineering, Siddaganga Institute of Technology, Karnataka, India
\(^{B}\)Department of Computer Science and Engineering, Siddaganga Institute of Technology, Karnataka, India

Abstract

Networks are distributed, and nodes spontaneously move from one network to another to access service in the ubiquitous computing environments. In these situations, adaptive security is systems require self-adaptive nature by monitoring the changes occurring in the operating environment and act accordingly at the runtime to overcome the security trade-offs. The adaptive security is achieved through continuous monitoring, observations, analysis and working adaptive security policies for the applications. This paper surveys adaptive security systems and evaluates critical security services (i.e. authentication, and authorization.). Based on our evaluation results, we provide future research recommendation in the ubiquitous computing environment.

Keywords: Policy, Trust, Taxonomy, Context, Adaptive Security, Ubiquitous Network

I. INTRODUCTION

A computing history [4] began with the centralized computing 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 [5] that are essential to realizing the ubiquitous computing vision of invisibility and ubiquity. This nature of ubiquity and mobility is in need of security issues including privacy, authentication, access control, 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 capacity of the device or security requirements reflecting towards changing network. There are no such works found which is aware of the deserved security level and define new security policy accordingly to the changing environment.

The characteristics of heterogeneity in operating application, network, and service require security in many ubiquitous environments including the smart spaces [8] and intelligent area. The necessary security in smart spaces of the ubiquitous computing and related technologies is achieved by considering the necessary adaptive mechanisms/policies [6]. The smart spaces include smart devices that are aware of the context in which they operate and adapt themselves to the new surroundings and requirements through security policies. A protection policy defined at the design time is not enough and cannot be considered to provide the security in the operational environment. Protection policy deployed automatically at run-time conquers much security to the current safety requirements of the environment [2]. The adopted security continue to protect valuable assets from harm, even when security concerns change dynamically based on the available context in the computing environment [3]. However, the security mechanism should be aware of the capacity and context of the device for computation to perform the analysis of the user behavior or environment. Thus, there is the need to focus the research on the adaptive security policies by considering the operating context through the trusted environment. From [7], adaptation does not only mean dynamic loading/replacement of software components or technologies but satisfying the requirements of application adaptation policies.

The security adaptation is not a new concept [1], it is the desirability of a system, which adapts security in an autonomous manner, to answer as quickly and efficiently to perceived security issues in the 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".

In our survey the security schemes based on adaptive policy generation for adopting security in the ubiquitous computing environment was reviewed and proposed a novel methodology to design an adaptive security framework.

The organization of the paper is as follows: section II introduces the motivation behind the review work, section III with the policy based security review, section IV with the context and trust based security policy system, and section V concludes the survey work.

II. MOTIVATION

In the current scenario, the context-aware systems have reached the real world from the working laboratories. This situation necessarily gives scope to [9] 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-

Many research works stressed the importance of context and trust based policy generation in the resource constrained ubiquitous computing environment. According to [13], 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. The changing computing resources, accessing services, network, contexts, and user trust characterized the ubiquitous environments a need for self-adaptive security policy [14].

Adaptive security methods can be classified by the utilized attributes in the design. The classification also considers how the security parameters are adapted for the new vulnerabilities in the ubiquitous environment. However, most of the security schemes limit the efficiency of a node by consuming a significant amount of node resources. Thus, the objective is to identify the adaptive security schemes and sub-classifies them by the effectiveness of security they offer in the resource constrained ubiquitous network.

From the Fig 1, the policies are based on various attributes. Among them, application based security policies provide procedures according to the requirement of the application. Further, the application security can depend on the service level or context based. The context based security policy can be defined once and continued accordingly or can dynamically change with the user context. The user context can depend upon the role he is playing in the environment. The policies are set according to the job hierarchy the user is playing in the organization or environment in which he is present. Besides these, the security policy can solely depend on the trust the user has gained in the operating environment. Other than the discussed categories, the security policies can be according to the application/environment security levels. Hence, all these categories contribute to design the security policies.

The policies are defined as rules governing choices in actions of the system derived from trust relationships, enterpriser’s goals and service level agreements. The disclosure of policies is again a security breach [16] that can hamper the whole system security when the policies are predefined. Hence, the policies are altered dynamically to endow security.

The translation of the adaptive policies from old to the new policy is achieved through ontology [19]. Ontology is represented like an administrator with the domain knowledge and security reasoning on best practice rules by creating desired configurations for network-level security controls (e.g., firewall and secure channels). An absence of automated reasoning for policy derivation and the usage of the human administrator always make the system non-adaptive. The system becomes partial adaptive when some access services using multiple channels. Though most of the channels assure secure communication, it is not practically remarkable. Hence, a well-managed context-aware security characterization of access services by adaptivity and multichannel access is much needed [21]. However, greater challenges were faced while developing frameworks to address security and privacy issues associated with the context-aware systems [22].

III. POLICY BASED SECURITY

A security policy according to [15], is defined as a set of rules for authorization, access control, and so on in the operating environments. Policies are usually defined to evaluate trust, context, available computing resource in devices and networks [17], and roles played in the computing environment. The security policies are also planned according to business needs while providing services or applications to render security in pervasive/ubiquitous/mobile networks. Hence, a clear stated specifications and goals [18] regarding adaptive security based on policies are concentrated in the ubiquitous security network.

The taxonomy of policy-based security in the ubiquitous computing system is given in Fig. 1. The figure shows the categorization of policies based on the operation nature, i.e., the policies can be predefined or adaptive while designing the security scheme/protocol.

![Figure 1: Taxonomy of policy based security](image-url)

Figure 1: Taxonomy of policy based security
Contrary to its contradictory nature, context awareness enhances the effectiveness of the mechanisms by incorporating contextual data into a decision-making process [23]. The context can be behavioral, computing or physical. Context is nothing but the information that defines the situation, status, environment, device capability, QoS (Quality of Service), availability and activity about an entity. Fig 2 and Fig 3 shows the detailed taxonomy of the context and trust respectively in the ubiquitous environment.

IV. SECURITY POLICY BASED ON CONTEXT AND TRUST

The idea of adaptive and ubiquitous systems is already a subject of intense research for several years to see context information as intellectual property to enforce security [20]. The technologies evolved nowadays enable users to Context-based security applied through policies express clear and concise practices [25]. An inclusion of context aware security through policies may be a guideline to design the framework. The security policies based on context gets on appropriate mechanism to enforce the required level of security for the existing or future situations. An access control models always try to use location and time as a context, but [26] used state/situation and relations between the entity as a context.

An Ontology-based Context-Aware Access Control based on policy model was considered for the context model. Except the inference of high-level implicit context information according to operator-defined rules and some performance overhead for access control, the work was appraisable.

Moreover, the policy based securities are adopted for centralized mechanism and rarely on the decentralized mechanism. The concept of the centralized approach used sharing of resources by the policy based secure communication.

Some of the works that are adaptive towards security using a centralized approach were reviewed and found some of the interesting things about context based security. The approach in [27] followed design specification and modifications without coding into automated agents. The policies defined could do with persistent and can be dynamically modified accordingly to change the system behavior without changing implementation (not new functionality). The [28] supported applications in a pervasive computing environment by presenting a software architecture adaptation for a set of mobile users accessing shared information through a variety of devices communicating over a heterogeneous communications infrastructure. The design uses queuing models and security analysis on policies with the performance modeling on mobile users with time-varying resources and heterogeneous devices. The work neglected to consider environmental context and trust about the user. Secure and trusted context information [29] was considered by the security policy enforcement in the dynamic environment.

The context-aware services raise a risk of security and privacy, but a straightforward approach keeps the risk behind. The usage of context [24] provides security as a primary attribute of the ubiquitous network, where the services more often are context-aware.

A context sensible policy based solution to secure access to service through service discovery in small scale and large scale ubiquitous computing environment will provide best adaptive security [30]. But, trust related issues [30] like trust evaluation or investigations about trusted party and how context is acquitted in the system is absent.

Figure 2: Taxonomy of Context
An attempt to combine centralized and decentralized approach [31] was done using the trust parameter for the e-commerce applications. Where, a policy based trust mechanisms are utilized for centralized approach and reputation-based mechanism for the decentralized approach. The work concentrated more on the verification of the source of information through authentication. The utilization of encryption and signature mechanisms delayed the performance and extravagant to computational capacity.

In the health care application, an adaptive policy definer and the manager consider the predefined context (critical, dangerous, and stable) for access control according to severity level. As per the required treatment, an administrator does not have the privilege to change the access related policy mathematically, but a specialist recommendation is most solicited in this situation. The proposal in [32] includes a context-driven trust to evaluate the authenticity of a user through adaptive security through the evaluation process. The complexity of trust computation level depends upon the security level. A consideration of the capacity of user’s device was neglected while computing the required level of security. Another proposal [33] was found to ignore the availability of computational resources. Here, the levels of trust are realized according to the user behavior, to access the application software based on experience, recommendation and knowledge-based. In [34], higher level trust requires more computational time and cost resulted in higher overhead. The proposal [33] also neglects to verify the capacity of the device while evaluating the authentication of a user. The policies for access control implemented in trust negotiation or for defining context priority [35] is based on available computational capacity. Ontology based information is used to determine the trust levels of the clients or for assigning trust rights in the given context. A testbed for an intelligence security system was created to test the efficiency of the work. The analysis shows to concentrate on security for acted actions, instead of working for each action on a large scale ubiquitous network communicated through heterogeneous devices and services. Finally, designing of the trust based security policies in the operating context was a major thought. To do so, a high level of flexibility, without a considerable loss of simplicity, was the central principle. A service-based application modeled and expressed in the form of self-adaptation policies [36] based on utility functions adopted context-aware security using the MAUT (i.e., MAPE model represented as MAUT) and GRBAC (General Role Based Access Control) in RFID/USN environments. The policies were defined according to the number of targets, requirements, applications and services available. In addition to this, the proposal [36] was adaptive to consider context integration with the detection and modification policies. The performance was compared with the Gaia.
[37] and Aura [38] with the security context. A negligence of security concern to context-aware service was found with the inclusion of heterogeneity below the lower level of an application layer.

The user behavior analysis using context variables of the environment and trust, to define an adaptive security policy for the information security management was the thought [39]. The security aspects of user behavior analysis and trust in behavior complimented the environmental context and biometric technologies as a base for defining an adaptive security policy. The policy set is defined to work in a flexible way by utilizing the trust and context of the human. This provided the proper approach to propose a context and trust based adaptive security policies for human behaviors. The involvement of self-adaptive nature will make any application or system more dynamic to security actions.

Work [40] focused more on need-to-know principle by using context and events to authorize subjects (users at the airport) to access data and physical objects (resources) on the activation of attribute based access control as security rules. Security rules depend upon the meta-rules defined while determining activation/deactivation of contexts. The risk modeling has been mapped to attribute based access control to identify vulnerabilities in the environment. The environmental information is found to be unbounded with the spatial information to make the model adaptive towards access control. Another user behavior based access control model using ontology is presented [41]. The access control is based on security policy formed from the prediction of future actions of dependent people using historical data, contextual data and user behavior data. The method used for user behaviors extraction and contextual data gathering was found to be absent in the approach.

An entity oriented security model based on trust assessment for e-Health system is proposed [42]. Here a novel set of trust assessment metrics was utilized to assess a particular property of a security system (i.e. partial metrics) or entire properties (i.e. total metrics) to make the model flexible in its approach and facilitates an entity trust depending on the contextual need. The architectural design of the trust assessment system was well structured with trust computation. These characteristics are well-guided approaches to non-generic and non-awareness towards environmental context.

From the above reviews, it was found that the security frameworks based on policies are becoming a hot research topic in the ubiquitous networks. The framework of security policies involved for evaluation of context and trust towards performance based on ontology may be one of the ideas for adaptive security. Otherwise, the security policies are designed for proper monitoring and collection of contextual and trust information’s and generation of security policies according to the required level is another criteria that suit well for the ubiquitous environment. Fig 5 shows the security design lifecycle based on context and trust to build an adaptive security policy. The policy generation according to the situation need makes the security framework adaptive and will be able to work efficiently regarding energy and time consumption compared to non-adaptive security framework.

IV. FUTURE WORK

The existing works never cover the whole process of providing the adaptive security. While designing adaptive security, many works in the field of ubiquitous are based on the trust and contextual information. A framework to gather operational environmental information, analyzing and planning the relevant security attributes are necessary for the heterogeneous world.

In future, the security policies for the today scenarios are to be adaptive by analyzing the changing situation. A runtime adaptive security policy is required while designing the framework. If adaptivity is not included, the static nature can create a route for the malicious activities. Hence, adaptive security policies are to be defined while providing the security to the applications in the ubiquitous network through proper monitoring, classification, planning and execution based on context and trust attributes.

Consequently, an additional research work is needed in the field of risk and threat management.

V. CONCLUSION

The world of heterogeneous network and devices do not drive with the regular static security policies. Hence, a dynamic policy nature is most required in the ubiquitous network, where the service and resources are shared and provided according to the user requirements.

This paper proposed a framework to design an adaptive security scheme that is based on contextual information and level of the trust the user is possessing in the ubiquitous environment. The framework also provides the automatic generation of right policy at the run time.

REFERENCES


