Novel Security Model for Pervasive Systems

S. Geetha.,
PG Scholar,
PEC, Pondicherry

G.Zayaraz, PhD.
Associate Professor,
PEC, Pondicherry

J. Madhusudanan
Research Scholar,
Pondicherry
University

V. Prasanna Venkatesan, PhD.
Associate Professor
Pondicherry Universit

ABSTRACT

As portable devices have become a part of our everyday life, more people are unknowingly participating in a pervasive computing environment. People might engage in many computational devices simultaneously without even the awareness of their existence. The idea of pervasive computing is that almost every device we see today will be capable of communication and function in collaboration with one another in the near future. Due to lack of a fixed infrastructure for authentication and authorization, devices in pervasive computing are more susceptible to malicious snoopers. In this paper, we cover different pervasive computing-based projects that have adopted pervasive middleware as an integral part of the security enforcement in their projects. We then move on to identify security requirements especially inherent to pervasive computing which makes it a smart security system. Finally, a security model for pervasive system is proposed that compose the required pervasive security functions to be smart.

Keywords

Pervasive computing, Pervasive security, Smart security. Security issues, Pervasive security architecture.

1. INTRODUCTION

Today's world is filled with various smart environments which makes us to allow achieving more smart services with the pervasive systems. The future pervasive computing environment will comprise a wide variety of devices and services from different manufacturers and developers. Therefore achieving platform and Vendor independence, architecture openness before making the pervasive computing spaces a common places is to be done. With such prevalence of pervasive technology, the interaction between portable devices needs to be continuous and imperceptible to users. The privacy of the information exchanged among the devices has become a critical issue with the different contexts of the environment. Like other systems, security and privacy are big concerns for the pervasive computing system. It was hoped that the intelligent environment would allow the effortless administration of the apparent complexity but we now understand that this will not happen and that in essence the environment is not really intelligent but it only appears intelligent when judged from the outside. A camera in the mobile phone is added with features like recognition of smile, etc., to make it smart but there is no smart security features in the existing pervasive systems. Though there is more smartness introduced in the pervasive systems how well it behaves smartly under various critical situations? Whether the security of the smart system is smart? These questions lead to the proposal of a smart security system for pervasive environment.

The Section 2 is a summary of the literature survey on Smart Systems. The Section 3 is about the identified Threats to Smart Systems. Section 4 is a summary on the Proposed Architecture. Section 5 shows an Example Scenario. Section 6 is a Cross cut of Smart aspects over traditional security. Section 7 summaries the proposed architecture. Section 8 shows a flow diagram for policy manager and Section 9 shows the flow diagram for Authenticator.

2. LITERATURE SURVEY

According to Jameela Al-Jaroodi et al. [1] Service-oriented computing aims to make services available and easily accessible through standardized models and protocols without having to worry about the underlying infrastructures, development models or implementation details. This helps achieve interoperability and loose coupling among distributed application components and also among user processes.

More trust models for pervasive systems have been proposed but they does not provide protection against malicious attacks and it fails to handle malicious situations when an user launches strategic attacks where the trust value is not modified due to that it considers the old behavior pattern. A frame work for interaction using trust in pervasive computing is been proposed but it has been not yet implemented with security aspects in it. Pervasive computing research field is still in its infancy. Lots of research is to be done to get the overall security of the pervasive systems. Although security schemes are derived to be implemented in the pervasive environment but they are being implemented into already existing pervasive computing architectures, so there is a lack in the security measures and they are specific for each applications. No generalized architecture exists in pervasive environment.

An extended survey is done to prove the need for smart security features in pervasive systems. As an example let us take the project of SWAMI (Safeguards in a World of Ambient Intelligence) [9]. The project is investigating the emerging challenges, in particular with respect to privacy, security, identity, trust and protection of rights for all

citizens in all their roles in the Information Society. SWAMI aims at identifying threats and system vulnerabilities and appropriate safeguards by developing and analyzing future scenarios, more precisely "dark scenarios", in order to analyze and understand future risks and vulnerabilities related to ambient intelligence.

Let us take another example [10], consider a slightly more complex scenario. Let ABC be a company that is providing Acme with contractual consulting services on the same temporary project that Mr.X is assigned to. Y and Z are employees of ABC and they have to report to Mr.X in McCoy about their project. Assume that y and z possess Id's which uses x.509 digital certificate which is issued by and signed by ABC's root certificate. This example necessitates that Mr.X will need to delegate certain rights to Acme systems and services to Y and Z for their temporary project.

The above said examples make us to think in a broader perspective to develop a security model which needs smart security features to handle various critical situations/context. According to the analysis done on existing smart system security it is clear that they are provided with security but not to the extent that it acts smartly in the event of conflicting contexts. Due to this lack in security features they become vulnerable to threats.

3. THREATS TO SMART SYSTEMS

Based on the survey done on smart systems it is identified that the smart devices and applications are vulnerable to various threats in the real time. According to Max Landman [16], the unusual mix of personal and business use for smart phones as well as their unique combination of capabilities creates a number of challenges to managing their risk.

According to Yuxin Chen, et.al, [11] however, smart appliances are not yet equipped with smart security protection mechanisms to defend against cyber attacks. They follow remote control commands without verifying the authenticity of such commands. In this context, if we introduce "smart" functions to electrical appliances without proper security protection, they become more vulnerable than conventional devices.

According to Petteri Alahuhta, et.al [9], human errors constitute major security weaknesses. Since not everything in the smart house will be accessed via biometric verification only, people will continue to use easy-to-guess or accessible passwords and/or access codes. Remote surveillance of the smart home is not enough to secure it. Security requires on-the-spot checks and back-up systems if something goes wrong.

According to Petros Belimpasakis and Vlad Stirbu [22], home network when attached to the public Internet, it is exposed to the threats of hackers and viruses. If these could gain access to the home network, they could control home devices, user content, and violate the privacy of the residents. These studies prove that the smart systems are with lack of security and are vulnerable to threats due to its open access and wireless communication network.

The various threats to the smart systems are listed below

- Privacy violations
- False trust or Distrust
- Data Laundering
- Man-in-Middle Attack
- Malicious Software Downloads
- Eavesdropping
- Sensor Brokers
- Direct hackers
- User behavior
- Cabir- a virus spread through Bluetooth
- Card Cloning
- Phishing
- Communication through wireless networks
- Denial of Service attacks.

4. PROPOSED WORK

The various security models for pervasive computing that has been developed till date is been implemented with the traditional security aspects like Confidentiality, Authentication, Authorization, Integrity, Privacy, etc., These security features are not enough for addressing the various issues in pervasive computing security, so we propose a novel security model which includes features like trust, autonomy, context-awareness, etc., that provide better security of the pervasive computing paradigm. The objective of the proposed work is to develop a security model for pervasive computing that provide a innovative security model to address the various issues in this field.

5. EXAMPLE SCENARIO

EXAMPLE	EXISTING SYSTEM	PROPOSED SYSTEM
Mr. X goes to a smart shopping mall he gets the information of various shops payment mechanisms through his smart phone.	The existing smart phone will check with the various security policies and due to limited security it will allow to connect with more shops.	This proposal will make the smart phone to assess the security policies of the various shops and suggests the suitable shops to purchase and infers the alternate policies for the remaining shops.

6. SMART ASPECTS IN SECURITY

Based on the literature survey it is identified that the existing security policies for pervasive system is with lack of features to provide a smart security. The proposal is to add features like autonomy, context awareness, intelligence to make the existing security system smarter. The below Table 2 illustrates the need of smart aspects.

TABLE: 2 Cross Cut of Smart Aspects with Security features

Traditional Security Features	Autonomy	Context Awareness	Intelligence
Authorization	YES [21][12]	YES [8][5]	NOT KNOWN
Authentication	YES [15][17]	NOT KNOWN	NOT KNOWN
Confidentiality	NOT KNOWN	NOT KNOWN	NO[18]
Cryptography	NOT KNOWN	NOT KNOWN	NOT KNOWN
Integrity	YES [4]	YES [2][3]	NOT KNOWN
Privacy	NOT KNOWN	YES [6][13]	NO[17][19]
Trust	YES [15][20]	NO [7][14]	NOT KNOWN

7. PROPOSED ARCHITECTURE

The objective of the proposed work is to develop a generic security model to provide better security to the pervasive systems. The architecture consists of context layer, Device layer, Security manager, autonomy Manager and Intelligent manager.

7.1 Context Layer

The Context Layer includes Context Manager to manage the various contexts of the applications. It uses the Context Handler to handle the contexts and Context Analyzer to analyze the contexts.

7.2 Device Layer

The Device Layer includes Device Manager to manage the various Contexts of the devices. The Device Clustering Manager is used to communicate between the various devices.

7.3 Security Manager

The Security manager includes an Authenticator to handle with the authentication policies. The Access Control Handler handles the various access control policies with the user. The Trust Manager manages the various trust related policies to provide different levels of access controls based on trust. The Privacy Handler handles the various privacy related policies The Cryptographic system manager and Confidentiality Handler is needed to check with policies of cryptosystems and the confidentiality of the data. The Policy Manager manages the various security policies and a security log is maintained to store the policy details.

7.4 Autonomy Manager

The Autonomy Manager includes Access Provider to provide access rights to the user. The Trust Handler will handle the various levels of user trust. The Conflict Context Handler (CCH) handles the various contexts and provides the needed policies for different contexts. The Policy Setter sets new policies when needed in case of conflicting policies and if there is no policy in the system.

7.5 Intelligent Manager

The Intelligent Manager includes an Access Evaluator to evaluate the various access control policies of the user. The Trust Evaluator evaluates the policies based on the user trust level. The Conflict Context Analyzer analyzes the various context policies. The Policy Analyzer will analyze the different policies of the system user.

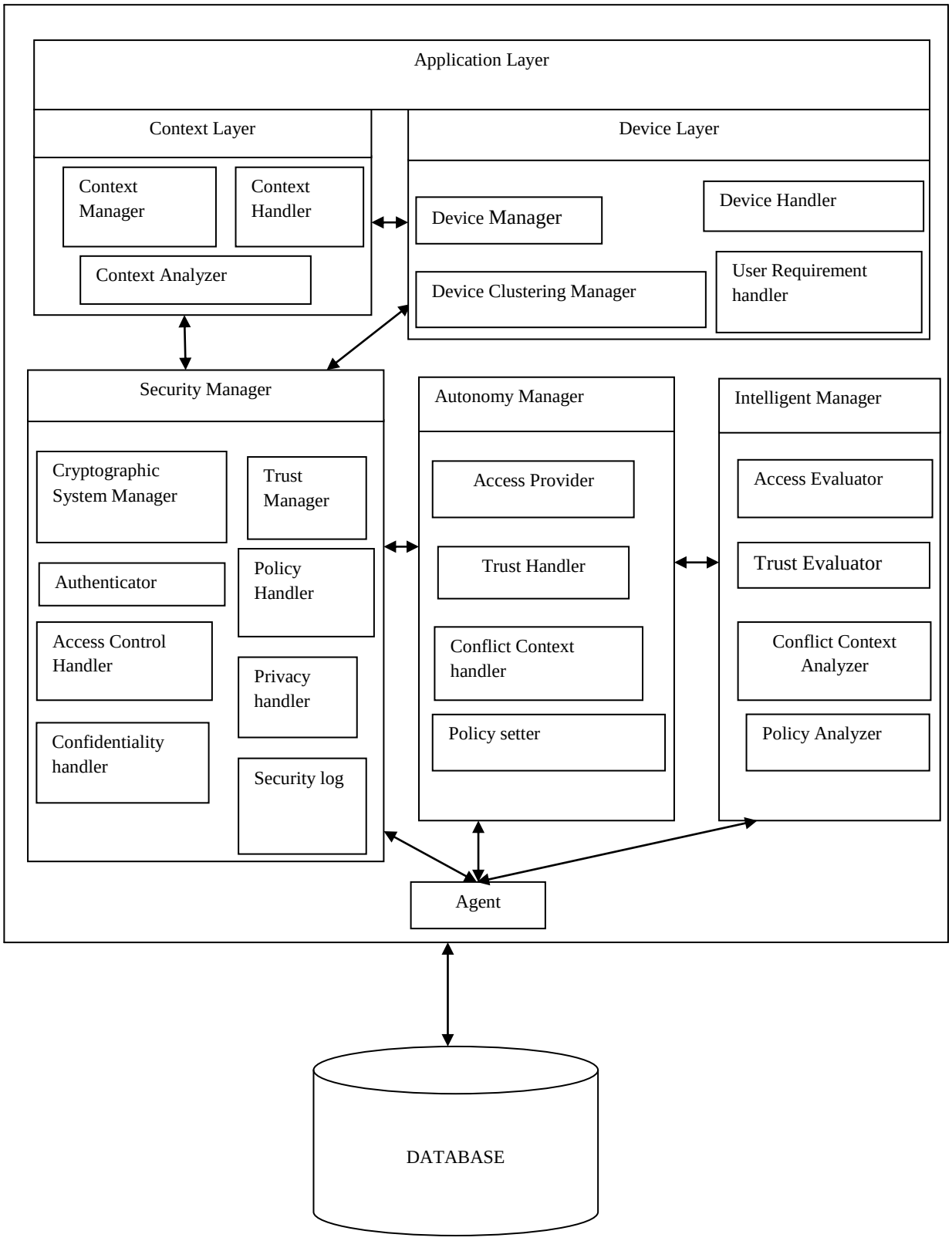

FIGURE 1: PROPOSED ARCHITECTURE

8 FLOW DIAGRAM FOR POLICY MANAGER

The Policy Manager checks for the security policies of the communicating device. If the policy is matched it allows accessing the device. If policy is not matched it checks for conflict in the policy, if conflict exists it gives it to conflict handler who analyses the conflicts and give it to policy setter. The policy setter will set new policies and give it the policy manager as shown in figure 2

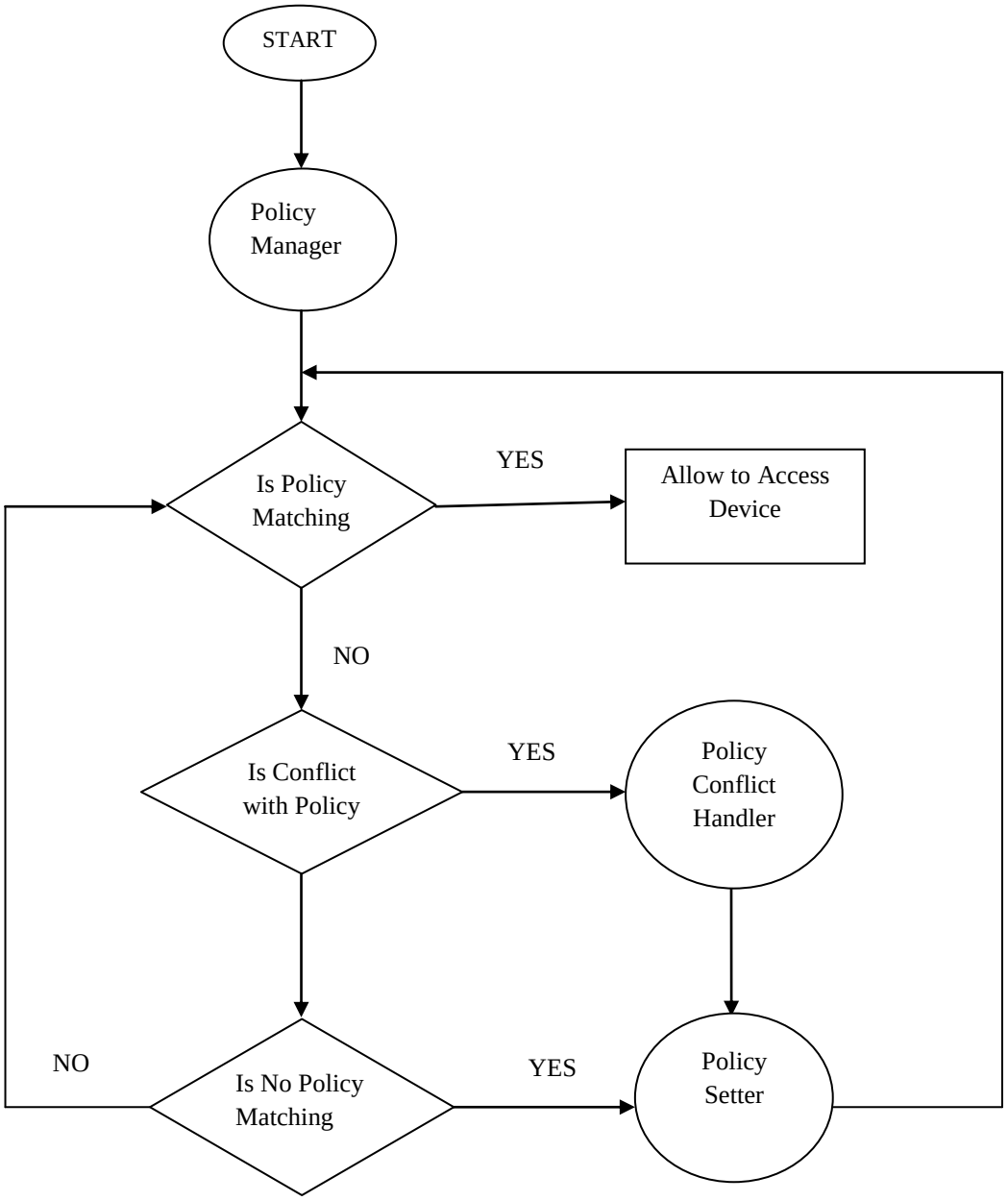

FIGURE 2: Flow Diagram for Policy Manager

9 FLOW DIAGRAM FOR AUTHENTICATOR:

The authenticator will check for the user authentication. If it is an unauthenticated user it sends it to policy analyzer to analyze the user authentication policies. The analyzer then gives it to Policy setter to set new authenticated policy for the user as shown in figure 3

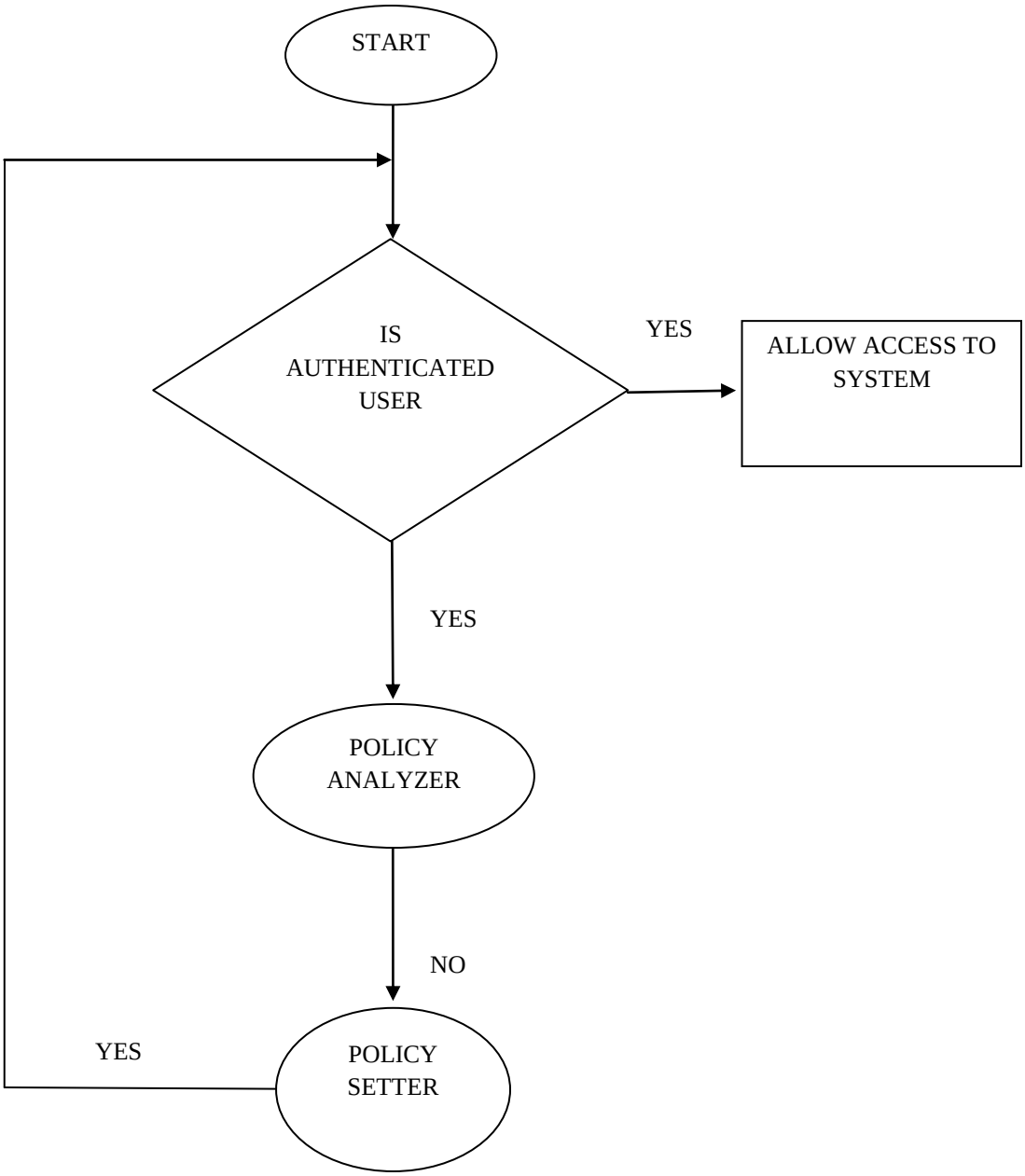

FIGURE 3: Authenticator Flow Diagram

10 CONCLUSION:

Pervasive computing security cannot be realized without sophisticated knowledge representation and reasoning and other AI and agent-oriented technologies. This work has been biased towards the second school of thought in the security of pervasive systems. Several concluding observations can be made from the proposed work. One, not surprising, is the universal agreement on the need for Context-awareness, Autonomy and Intelligence in the security of the pervasive systems to make it a smart security. In this paper, a review about the various security approaches in pervasive computing is been done. Based on the different approaches and survey on threats it is clear that the existing smart system is with lack of smart security aspects. So a security architecture for pervasive systems with smart aspects is been proposed to provide a novel security policies for the smart systems.

11 REFERENCES:

[1] Al-Jaroodi, J., N. Mohamed, and J. Aziz, "Service Oriented Middleware: Trends and Challenges," in proc. 7th International Conference on Information Technology: New Generations (ITNG), IEEE CPS, Las Vegas, USA, April 2010.

[2] Sheng-Tzong Cheng, Chi-Hsuan Wang : "An Adaptive Scenario-Based Reasoning System Across Smart Houses", Journal Wireless Personal Communications, Volume 64, December 2010.

[3] Jiehan Zhou, et al. " Context-aware pervasive service composition and its implementation", Journal Personal and Ubiquitous Computing, Volume 15, 2011.

[4] Toma´s Sa´nchez Lo´pez, Damith C. Ranasinghe, Mark Harrison, Duncan McFarlane: "Adding sense to the Internet of Things-An architecture framework for Smart Object systems", Journal Personal and Ubiquitous Computing, Volume 16, 2012.

[5] Montanari.R, Tibaldi.D, Toninelli.A : "A Context-Centric Security Middleware for Service Provisioning in Pervasive Computing", Applications and the Internet, 2005 Proceedings, IEEE Conference, pages 421-429.

[6] Achilleas Achilleos, Kun Yang, Nektarios Georgalas: "Context Modelling and a Context-aware Framework for Pervasive Service Creation: A model-driven approach", Journal on Pervasive and Mobile Computing, Volume 6, April 2010, pages 281-296,ScienceDirect.

[7] Daniele Miorandi, et al. "Internet of Things: Vision, applications and research challenges", Journal on Ad Hoc Networks, Volume 10, Issue 7, September 2012, pages 1497-1516.

[8] Patroklos G. argyroudis, Donal O' Mahony: "Towards a context-aware framework for pervasive computing authorization management", Proceedings of 3rd UK-UbiNet Workshop: Designing, Evaluating and Using Ubiquitous Computing Systems, Bath, UK, February 2005.

[9] Petteri Alahuhta, et al. "SWAMI- Dark scenarios in ambient intelligence: Highlighting risks and vulnerabilities ", Information Society Technologies, Sixth frame work Programme, January 2010.

[10] Lalana Kagal,et al.: " Vigil : Providing Trust for Enhanced Security in Pervasive Systems ", IBM EECOMS program, the DARPA DAML program under contract F30602-97-1-0215,and by NSF through awards CCR0070802, IIS9875433.

[11] Yuxin Chen, Bo Luo: " S2A: Secure Smart Household Appliances ", CODASPY'12, San Antonio, Texas, USA, ACM 978-1-4503-1091-02/2012.

[12] Anand Ranganathan, et al. "A Middleware for Context-Aware agents in Ubiquitous Computing Environments". GAIA Project 2003. http://choices.cs.uiuc.edu/gaia/ papers/

[13] Susana Alcalde Bagues, Andreas Zeidler: "Sentry@Home-Leveraging the smart home for privacy in pervasive computing", International Journal of smart home, Volume 1, July 2007.

[14] Karl Krukow, Mogens Nielsen and Vladimiro Sassone: "Trust Models in Ubiquitous Computing", Philosophical transactions of the Royal Society A, Volume 366, pages 3781-3793, August 2008.

[15] Anas El Husseini, et al. "Trust-based authentication scheme with user rating for low-resource devices in smart environments": Journal of Personal ubiquitous Computing, Volume 8, Springer Publications.

[16] Max Landman: "Managing Smart Phone Security Risks ", InfoSecCD'10, 2010, Kennesaw, GA, USA, ACM 978-1-60558-661-8/10/2010.

[17] Wei-Wei Ni er, Jin-Wang Zheng, and Zhi-Hong Chong: "HilAnchor: Location Privacy Protection in the Presence of Users' Preferences", JOURNAL OF COMPUTER SCIENCE AND TECHNOLOGY, volume 27, pages 413-427, March 2012.

[18] Akihiro Eguchi, et al."Everything is alive: Towards the future wisdom web of things",Journal of World wide web, Volume 4 , 2012.

[19] E Toch "Personalization and privacy: A survey of pervasive risks and remedies in personalization based systems", Journal of User Model User - Adaptive Internet, volume 22, pages 203-220, 2012

[20] Lalana Kagal, Jeffrey Undercoffer, Filip Perich, Anupam Joshi, Tim Finin:"A security architecture based on trust management for pervasive computing systems", project supported by NSF Awards IIS and the Defense Advanced Research Projects Agency.

[21] Intae Kim, Daesung Lee, Kuinam J. Kim , Junghyun Lee: "Flexible authorization in home network environments", Journal Cluster Computing, Volume 15 Issue 1, March 2012.

[22] Petros Belimpasakis, Vlad Stirbu: "A survey of techniques for remote access to home networks and resources ", Journal on Multimedia Tools and Applications, Springer, September 2012.