Recent Trends in Intensive Computing
M. Rajesh et al. (Eds.)

doi:10.3233/APC210193

Pervasive Computing Applications and Security – A Deep Insight

S. Magesh [a,1], Sujatha Jamuna Anand [b], Niveditha V.R[c], Y. Pavan Kumar Reddy [d], P.S. Rajakumar [c]
[a] Maruthi Technocrat E Services, Chennai, India
[b] Loyola Institute of Technology, Chennai, Tamil Nadu, India
[c] Department of Computer Science and Engineering, Dr M.G.R Educational and Research Institute, Chennai, India
[d] Geethanjali Institute of Science and Technology, Nellore, Andhra Pradesh, India

Abstract. Pervasive computing has made life easy with communication devices. Today devise collaboration has enhanced everywhere in this environment. It has made computing devices invisible and the services. This pervasive framework provides applications with interactions, numerous cooperation and accessibility, and integration. The proposed work enumerates the applications, pervasive security challenges. It provides security predicaments by assigning certificate credentials, access controls, trust management, and some security techniques to overcome the security paradigms in these distributed networks with IoT and the pervasive computing framework. The work also encounters security perplexities in handling the security threats and user interaction issues. Nevertheless, security techniques are listed for various pervasive applications in distinct domains such as healthcare, industries, and transforming sensitive information. The smart applications with smart environments perhaps force towards the new technologies in the pervasive computing outlook. The work also embedded with middleware with the context-based situation in these pervasive applications

Keywords. Pervasive computing, Pervasive security, Certificate credentials, distributed networks, trust management.

1. Introduction

Pervasive computing has become the growing trend of embedded computing systems and promoted with smart technologies such as smart health, smart home, smart environment in our everyday entities [1]. This pervasive environment provides effective communication and performs efficient tasks to minimize the end user's need to interact with computing technologies [2]. It can be accessed irrespective of the environment across any network handling different tasks from one node to another as it is portable. Pervasive computing systems are connected in a heterogeneous network environment everywhere with every smart device [3]. Pervasive computing has its potential in various domains such as defense, finance and healthcare. As these domains are accessing through laptops, personal digital assistants (PDA) and other smart devices, there are various difficulties at various levels [4]. According to Mark Weiser's point of view [5,6], pervasive computing is said to the next generation computing

[1] S. Magesh, Maruthi Technocrat E Services, Chennai, India,
Email: mageshmtech@gmail.com.

environment provided with communication anywhere at any time for anybody. The proposed work is focused on

- Pervasive Applications in various domains with convenient access.
- Assigning security credentials to every individual deploying pervasive devices.
- Security attacks and security requirements to access the device correctly allow authorized access to modify access rights to third parties.

2. Pervasive Environment and Applications

Pervasive computing has simplified human lives in day-to-day activities by providing Smartphone users to carry out their tasks through portable and embedded computing devices. In recent days, pervasive computing has entirely changed the lifestyle while interacting with information. The multiple connected devices, as well as the environment, had demanded robust and secured information systems. These systems are embedded with various network hubs providing continuous and reliable connectivity with smart devices in an IoT environment. It focuses on sensor data providing better communication with both mobile and distributing environment [7]. The pervasive computer architecture of sensors and embedded devices is represented in **Figure 1** with various sensors embedded with IoT applications connected with low-cost device including the mobility service and connectivity. Tablets, smartphones, smart homes, wearable devices, and sensors have all evolved due to the pervasive environment.

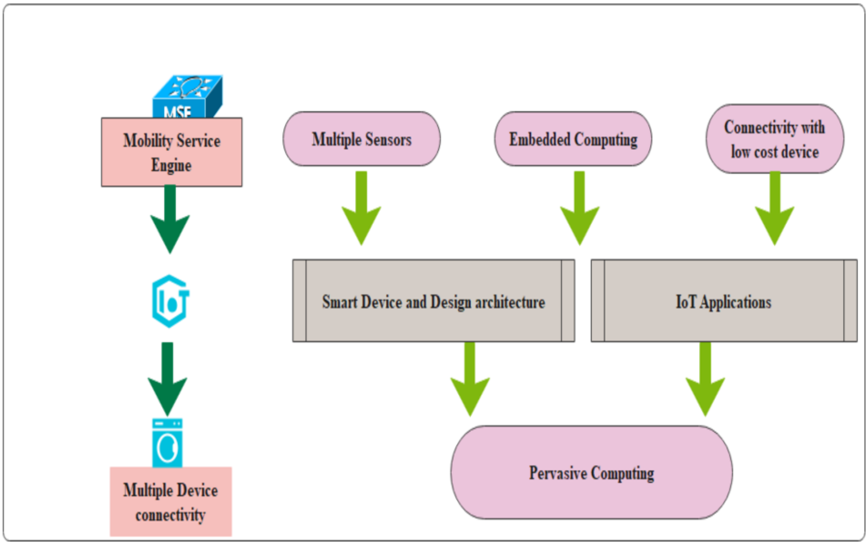
MSE
Mobility Service Engine
Multiple Sensors
Embedded Computing
Connectivity with low cost device
Smart Device and Design architecture
IoT Applications
Multiple Device connectivity
Pervasive Computing

Figure 1. Pervasive Computing Environment

From simple tasks like switching the lights in the workplace, lecture and convention rooms, office cabins, and updating their emails to more complicated tasks like booking plane tickets, stock purchasing and sale, and managing banking accounts, this world has made life more accessible to the humans. By integrating these smart devices with smart environment, a new environment is launched, supporting any device with any environment that produces the pervasive environment **(Figure 2)** representing various smart devices in smart environment.

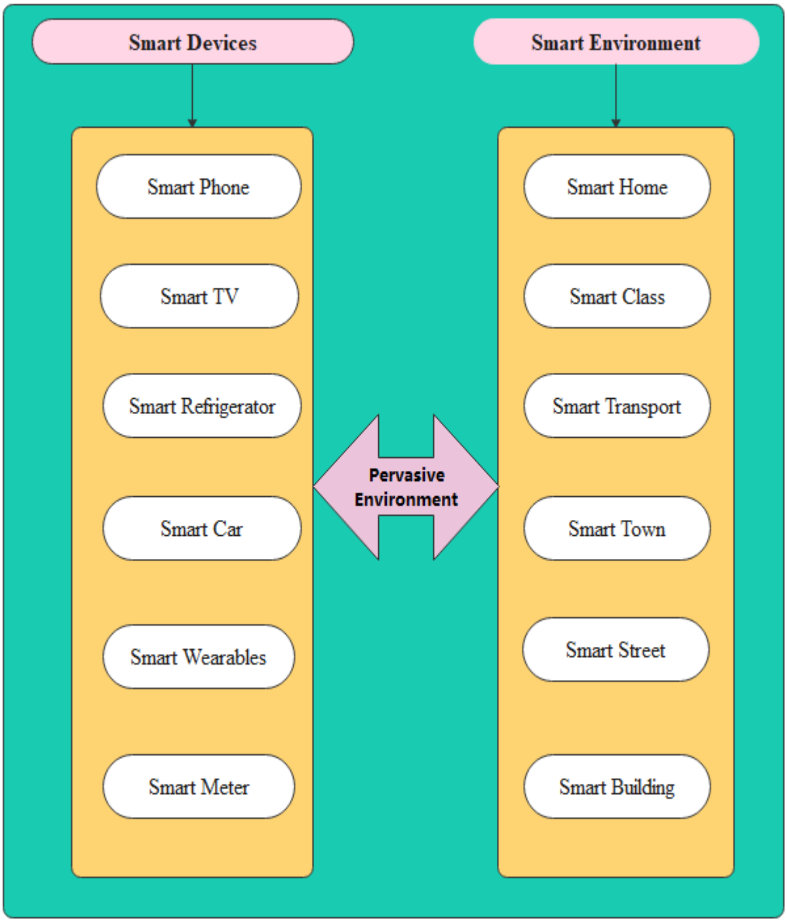

Figure 2. Various Applications of Pervasive Computing

3. Security Challenges in Pervasive Environment

Providing security to such a widely distributed model leads to face many challenges at a certain level. This can be related to a scenario like a person who does not belong to the enterprise has access to that concern. There are several problems in providing security in this pervasive environment. The significant challenges identified are change of user data, hacking client-server information, eavesdropping, privacy loss, smart device theft, stealing sensitive data, memory isolation, data forgery, original data alteration, economic issues, utilization of unpermitted connection, exploiting sensitive data. Few additional issues on protecting the system are as follows:

- **Inconspicuous and Invisibility**: Generally, the pervasive computing seems to be unnoticeable as data are sent and received daily. This diminishes the environment making easy acceptance that paves the way for attacking the user privacy.

- **Creation of Smart Spaces**: Sensors and other devices are integrated to sense, analyze and learn every area. It is also tractable that leads to getting the user's intention with privacy risks.
- **Other Privacy Issues**: Augmentation of dynamic spaces with actuators and sensors has provided brilliant spaces and computing efficiency. The utilization of different sensors and devices with dynamic space customized for users could cause a serious vulnerability to privacy, and malicious attackers and intruders can mislead this gap. Specific security attacks also affect the pervasive environment [8]. Those attacks include attacks due to modification, impersonation, and flooding attacks. **Figure 3** addresses some of the main issues in pervasive security.

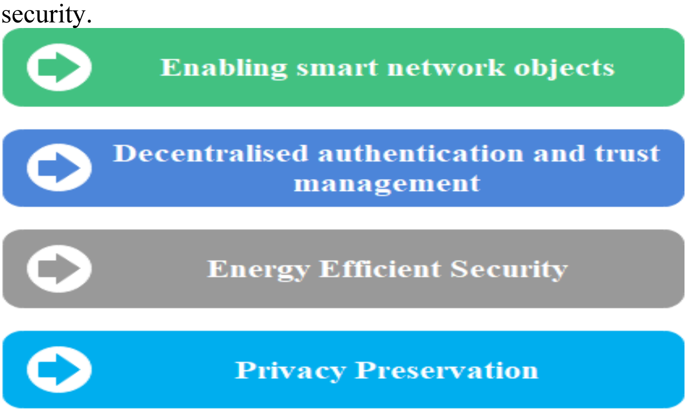
Enabling smart network objects
Decentralised authentication and trust management
Energy Efficient Security
Privacy Preservation

Figure 3. Security issues in Pervasive Environment

- **Attacks due to Modification**: In these attacks, packet headers are modified by sniffers and affects the integrity and the availability of the message [9].
- **Attacks due to Impersonation**: This is one type of eves dropping, providing integrity issues. It is classified under ARP spoofing attacks [10] that masquerades the connected device's destination address, and a duplicate MAC address is inserted.
- **Flooding Attacks**: Unwanted or undesired messages are sent frequently to their neighbor nodes, causing overhead. Dos, Routing Table overflow are classified under these attacks.

4. Security Predicaments

Pervasive security is an essential security technology to promote the progress of security program, including policies. The requirement of pervasive security is described below:

- **Clarity with compliance:** the main aim of security implementation is to ensure compliance by monitoring and improving users at a higher organization. In this context, security needs to be more apparent without causing aggravation to the users.
- **Managing Security Policies**: Providing a delegation certificate is an essential security requirement for access privilege. The security agent is responsible for controlling the service. At the user's request, the security agent transmits the credential with a delegation or ID certificate. The agent may also generate an

authorization certificate to use as tickets for accessing the resource. **Figure 4** shows the pervasive scenario in the health monitoring system illustrating the acquisition of patient’s database using the sensor network, filtering the data using preprocessing methods, analyzing the data using queries and then diagnosing accordingly.

- **Ensuring Multilevel Layer:** The security architecture should ensure security services at different levels within the available resources, strategies, domain and context middleware.
- **Interoperability and Scalability:** Utilization of various security technologies in recent years, multiple security measures need to be implemented, and security services need to be designed so that it needs to be portable and accessible at all levels providing inbuilt devices. Besides encoded actions, delegations and privileges, an open environment built on an XML framework named DAML (DARPA XML) Agent are well suited in an open environment. A security tool named Diasuite allows defining the taxonomy of a particular application with prewritten specification [11]. The privacy of the users can be protected by replacing X.509 signatures, including the authorized person's designation.

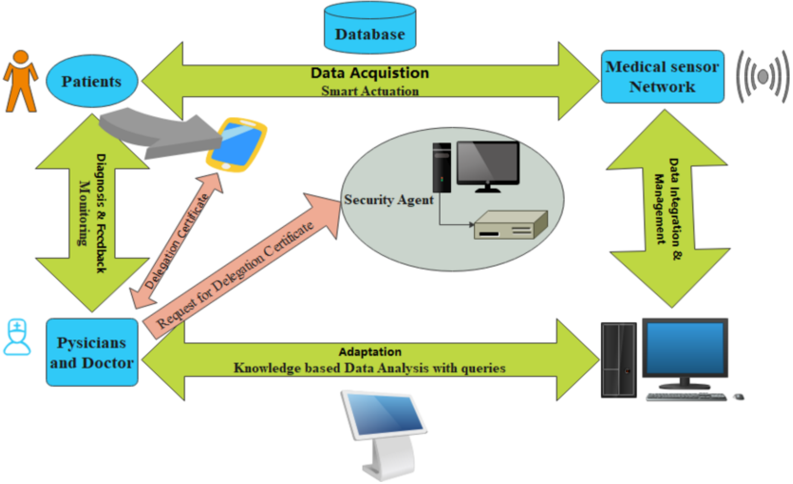
Database
Patients
Data Acquistion
Smart Actuation
Medical sensor Network
Diagnosis & Feedback Monitoring
Security Agent
Delegation Certificate
Request for Delegation Certificate
Data Integration & Management
Pysicians and Doctor
Adaptation
Knowledge based Data Analysis with queries

Figure 4. Health care Monitoring in Secured Pervasive Environment

The security predicaments need to ensure the security challenges such as Authentication and access control Confidentiality Integrity and Availability. Authentication and access control are the two security aspects to be ensured for every specific user.

5. Discussions

Pervasive security is simply establishing the quantitative and qualitative parameters by defining the reliability, topology, some failure patterns and efficiency in designing the architecture. Specific user-centric parameters need to evaluate to monitor the system's behavior towards the intension of the users' expectations and how the system takes efforts on the users' part relying on the system. Pervasive security works everywhere, irrespective of the network resources for data transmission. The entities such as business, technical and policies need to be secured. Today Pervasive computing has expanded transparently in many environments. Providing protection against unauthorized users, preventing access by unverified methods, accessing facilities and denial of service for unauthenticated users are some of the services rendered by Pervasive computing.

6. Conclusion

Today security for pervasive computing has become a complicated paradigm than exploiting the pervasive environment. The proposed study discusses the application of smart devices in a pervasive environment, pervasive security challenges and privacy issues. To overcome those paradigms, the study also enumerates some pervasive security requirements and provides solutions to security attacks by evaluating the security parameters in the pervasive environment. The main focus of the paper lies in the security issues in the smart environment and addressing the security predicaments in the distributed environment. Nevertheless, smart devices are deployed by many domains with ease and comfort. Due to its insecurity, higher-level protocols need to be enhanced in the environment soon.

References

[1] Ahmed, A.W., Ahmed, M.M., Khan, O.A. and Shah, M.A., 2017. A comprehensive analysis on the security threats and their countermeasures of IoT. International Journal of Advanced Computer Science and Applications, 8(7), pp.489-501.

[2] AbdAllah, E.G., Hassanein, H.S. and Zulkernine, M., 2015. A survey of security attacks in information-centric networking. IEEE Communications Surveys & Tutorials, 17(3), pp.1441-1454.

[3] Usman, A.B. and Gutierrez, J., 2018. Toward trust based protocols in a pervasive and mobile computing environment: A survey. Ad Hoc Networks, 81, pp.143-159.

[4] Hooda, M., Pathak, S. and Yadav, B., 2017, September. Pervasive Security of Internet Enabled Host Services. In 2017 International Conference on Current Trends in Computer, Electrical, Electronics and Communication (CTCEEC) (pp. 784-789). IEEE.

[5] Bdiwi, R., De Runz, C., Faiz, S. and Cherif, A.A., 2017, July. Towards a new ubiquitous learning environment based on blockchain technology. In 2017 IEEE 17th International Conference on Advanced Learning Technologies (ICALT) (pp. 101-102). IEEE.

[6] Dharminder, D. and Mishra, D., 2020. LCPPA: Lattice-based conditional privacy preserving authentication in vehicular communication. Transactions on Emerging Telecommunications Technologies, 31(2), p.e3810.

[7] Gollagi, S.G., Math, M.M. & Daptardar, A.A. A survey on pervasive computing over context-aware system. CCF Trans. Pervasive Comp. Interact. 2, 79–85 (2020).

[8] Naik, A.S. and Murugan, R., 2018. Security attacks and energy efficiency in wireless sensor networks: A survey. International Journal of Applied Engineering Research, 13(1), pp.107-112.

[9] Ladas, A., Deepak, G.C., Pavlatos, N. and Politis, C., 2018. A selective multipath routing protocol for ubiquitous networks. Ad Hoc Networks, 77, pp.95-107.

[10] Bdiwi, R., De Runz, C., Faiz, S. and Cherif, A.A., 2017, July. Towards a new ubiquitous learning environment based on blockchain technology. In 2017 IEEE 17th International Conference on Advanced Learning Technologies (ICALT) (pp. 101-102). IEEE.

[11] Cassou, D., Bruneau, J., Consel, C. and Balland, E., 2011. Toward a tool-based development methodology for pervasive computing applications. IEEE Transactions on Software Engineering, 38(6), pp.1445-1463.