ST. MARY'S UNIVERSITY

FACULTY OF INFORMATICS

DEPARTMENT OF COMPUTER SCIENCE

A GENERIC MULTI-TIER PRIVACY MODEL PREFERENCE SELECTION (GM-PMPS) IN A PERVASIVE ENVIRONMENT

BY: BINIYAM ABEBE

JULY 2020

ADDIS ABABA, ETHIOPIA

A GENERIC MULTI-TIER PRIVACY MODEL PREFERENCE SELECTION (GM-PMPS) IN A PERVASIVE ENVIRONMENT

BY

BINIYAM ABEBE

to

Faculty of Informatics

of

St. Mary's University

In Partial Fulfillment of the Requirements

For the Degree of Master of Science

in

Computer Science

Advisor: Asrat Mulat (PhD)

July 2020

ACCEPTANCE

Accepted by the Faculty of Informatics, St. Mary's University, in partial fulfillment of the requirements for the Degree of Master of Science in Computer Science

Thesis Examination Committee:

_____

Advisor

Asrat Mulat (PhD)

_____

Internal Examiner

million

_____

External Examiner

_____

Dean, Faculty of Informatics

July 2020

Declaration

I, the undersigned, declare that this thesis work is my original work, has not been presented for a degree in this or any other university, and all sources of materials used for the thesis work have been duly acknowledged.

Biniyam Abebe

Full Name of the Student

_____

Signature

Addis Ababa

Ethiopia

This thesis has been submitted for examination with my approval as advisor.

Asrat Mulat (PhD

Full Name of the Advisor

_____

Signature

Addis Ababa

Ethiopia

July 2020

Acknowledgements

With all due respect, this work would not have been possible without the genuine and dedicated guidance of my advisor, Dr. Asrat Mulat. I am deeply grateful for his unwavering support and mentorship, which were instrumental in shaping this research and making it clear and impactful.

I would also like to extend my heartfelt thanks to my family and friends for their continuous support and understanding throughout my research journey and the writing of this paper. Their encouragement kept me motivated during challenging times.

Finally, I give all glory to Almighty God, who sustained me through every difficulty. I have felt His guidance daily, and it is by His grace that I have completed this degree. I will continue to trust Him for my future.

Biniyam Abebe

Abstract

Pervasive computing is an emerging computing paradigm expected to become part of our everyday lifestyle in the foreseeable future. Despite its dynamic nature and high demand for information, many drawbacks and undesirable use in terms of privacy can be foreseen. More precisely, the pervasive computing paradigm raises concerns about end-user privacy, and ensuring privacy is becoming a major challenge requiring a tradeoff between privacy and context-aware service adaptation. This research work proposes a generic multitier model for end-user privacy preference selection to handle possible malicious requests through a predefined "aura" configured and controlled by users via privacy preferences. The multitier model is structured around users' natural relations, categorized as personal, social, and third-party aura, which can be evaluated in a group for any privacy-related requests based on trust accumulated through formulated and archived reputations. Since the exchange of local trust is the basis for determining reputation, the necessary trust value is determined by the weighted average result of a reputation figure gathered from direct and indirect request responses of nodes within the established aura. Finally, the implemented prototype of the proposed model determines the trust level of the requesting node based on the user's privacy preference selection bias point for the service and decides whether to respond automatically, require manual intervention, or block the request.

Keywords: Generic Multitier Aura, Reputations, Trust, Privacy Preference Selections

List of Acronyms

DDoS ----------Distributed Denial of Services

IoT ----------Internet of Things

MANET -------- Mobil Ad hoc Network

PCE ----------Pervasive Computing Environment

PEM ----------Privacy Enhancing Model

PET ----------Privacy Enhanced Technology

PII ----------Personal Identifiable Information

SDN----------Software-Defined Networks

UPEM ----------User-centered Privacy Evaluation Model

List of Figures

Table of Contents

Chapter One

1. Introduction

1.1. Background

While computers truly emerged as transformative inventions in the late 20th century, their conceptual origins trace back over 2,500 years to the abacus—a bead-and-wire calculator [1]. Though the technological gap between ancient abaci and modern computers appears vast, their shared principle remains: performing repetitive calculations faster than the human brain. Yet it's remarkable that this basic tool not only pioneered numeric encoding but also indirectly laid the groundwork for today's internet-driven computing revolution, which now permeates every aspect of daily life.

Computer technology is evolving not only in its widespread use but also in overall design and function [1]. The emergence of the Internet of Things (IoT) has led to pervasive connections among people, services, sensors, and objects. IoT devices are now deployed in a wide range of applications, from smart grids to healthcare and intelligent transport systems [2]. Today, there is not a single bit of astonishment that the evolution of computers continues to at an unprecedented pace. Technologies are being developed using small, relatively inexpensive, wireless-enabled computers that may lead to the near-omnipresence of information gathering and processing—a trend called pervasive computing. The miniaturization of processors and sensors enables an array of devices that can be embedded in clothing, appliances, carpets, food packaging, doors, windows, paperback books, and other everyday items, gathering data about when, how, and possibly by whom an item is used. While the era of pervasive and ubiquitous computing offers exciting potential and practical applications for commerce, healthcare, and other fields, the fine-grained data collection and widespread potential for misuse raise ethical concerns regarding individual privacy, security, and unforeseen issues [3].

In this section, concepts around pervasive computing is presented to help researchers better understand its nuts and bolts, which will aid in comprehending the proposed model to be discussed in subsequent chapters. The review follows a discussion flow from general concepts to specific

details. Here, pervasive computing, context-aware environments, multi-tier privacy, and preference selection are examined one by one.

1.1.1. Pervasive Computing

The evolving definition of connectivity has given rise to a new paradigm being implemented across multiple domains: the Pervasive Context-Aware Environment. Pervasive computing embeds distributed computational capabilities into everyday objects, enabling wireless intercommunication. Traditional computers will recede into the background - becoming minimally visible and intrusive - while maintaining dynamic connections within this pervasive ecosystem. As noted by [4], the most transformative technologies are those that become invisible, seamlessly integrating into daily life until indistinguishable from it.

The term pervasive computing emerged from research at IBM during 1996-97, embracing the vision of computing services available anytime, anywhere and on demand [5]. Pervasive Computing refers to the emerging trend toward: numerous, casually accessible, often invisible computing devices, frequently mobile or embedded in the environment, connected to an increasingly ubiquitous network infrastructure composed of a wired core and wireless edges [6]. Mark Weiser [4] discussed that for a technology to be really ubiquitous it should become a part of the fabric of our everyday life. Thus, the main objective is to use omnipresent devices with computational and communication capabilities that function gradually, modestly, and which are used instinctively by end-users.

Pervasive computing mainly consists of three set of entities: user agents (i.e. devices carried by users), devices embedded to the environment and the internet [4]. The digital interaction in between these entities would enable new applications. Based on the interaction mode a pervasive computing application classified into three categories, like user agent to user agent, user agent to internet and user agent to smart environment [6].

Eventually there are four primary research challenges facing to a pervasive computing that need to be addressed through time. These embraces minimization of human involvement and simplification of human – computer interaction, judicious use of limited battery lifetime on mobile devices, data privacy and spontaneous interaction between device through wireless interfaces [6].

1.1.2. Context Aware Environment

A Context is any information that can be used to characterize the situation of an entity that is considered relevant to the interaction between a user and an application, including the user and the application themselves [7]. It is generally identified as a proxy for interest, which is to mean that a gateway to turn on human attention, and since the most valuable resource in today's computing is identified as that (i.e., human attention), it has led to the inception of context-aware computing as its counterpart, which is mostly explained in the subsequent manners.

Context aware computing is a mobile computing paradigm in which applications can discover and take advantage of contextual information such as user location, time of day, neighboring users and devices, and user activity [8]. A system is considered to be context aware if it utilizes and provide the appropriate information or service to the user where appropriate and significant information depends upon the requirement and need of a user [9]. Users can take decision based upon the context information themselves or configure their handheld context aware devices to take intelligent decision on their behalf. This facilitates computer use for a wealth of new and diverse applications [10].

Basically, there are three important aspects that engaged under context environment: where you are; who you are with; and what resources are nearby [7]. Although location is a primary capability, location-aware does not necessarily capture things of interest that are mobile or changing. Context-aware in contrast is used more generally to include location, nearby people, time, devices, noise level, network availability, and even the social situation [7].

Thus, based on the observation of the real-world scenario of todays' life style, context aware application can be implemented on very diverse kinds of computing platforms, ranging from handheld devices to wearable computers to custom-built embedded systems. The goal of context information acquisition should be to determine what a user is trying to accomplish in aspects of context user's location, the user's neighbor, and resources near the user which is all subject to changing execution environment. However, there is divergent opinion as to whether context should only comprise automatically or manually acquired. In an ideal setting context would be obtained automatically but in real world context information can be recognized automatically and also though an application that accept and process a users' interventions. Nowadays ubiquity is somehow fully embedded, with smart devices integrating intelligence for processing various kinds

of data. Some of the approaches for acquiring context information are addressed by direct sensing and context server. Though this is realized through built-in local sensors which enable to gather the desired level of information directly and using a context server which is multiple clients are permitted to access to remote data sources. One of the most exciting aspects so far, future will involve the integration of computing and communication into mobile and dynamic environment [11]. This as a result would prove the significance of context aware computing when realized on a full scale. It will have a much greater impact on the quality of life for the user.

1.1.3. Privacy in Pervasive Environment

Information is the hub of today's interconnected societies [12]. We need to be able to exchange and retrieve our personal information quickly, efficiently, and securely, at any time and regardless of our current physical location. Recent years have seen the confluence of two major trends - the increase of mobile computing devices such as smart phones as a primary access point to networked information and the rise of social media platforms that connect people [12]. This indicates a basic fact that the next generation computational settings will be pervasive. Though in order to gain wide scale acceptance and adoptions from the direct and indirect users such critical issues of privacy under pervasive must be improved and solved.

Privacy is a fundamental human right. Life without privacy would a living hell. Information Privacy is the right and the ability of individuals to exercise control over the collection, use, and disclosure of their personal identifiable information (PII) to other individuals to express them selectively [13]. The PIIs can be biographical, biological, transactional, location or any other information that can be used for tracing or distinguishing the user identity [4].

The ubiquitous and pervasiveness improves the user comfort level, but also makes user PIIs highly prone to leakage. [14] Ensuring users' privacy is becoming a major challenge in context-aware applications. As mobile applications increasingly rely on automatic sensing to simplify and personalize services to users, users may find it difficult to trust the process in which services collect and use their context information. Users need to know that their information is collected and used in a way which is consistent with their expectations [15].

The protection of privacy and pervasiveness at the same time is by its very nature somewhat contradictory. Due to the fact the main characteristics of pervasive computing even tells being

ubiquity, invisibility, sensing, interconnectivity and cooperation between participating devices and memory amplification make the challenge even worsen [1]. These appearances with omnipresence and invisibility of devises in pervasive environment stress the importance of privacy issues in a pervasive computing. For example, the surveillance and data collection of participating devices will automatically pose a serious threat to privacy. In addition, this environment will sense, collect, store and share large amount of personal data in order to course information collection, processing and sharing is a fundamental requirement for the appropriate operation of such systems, though again we need to stress privacy issues under pervasive environment. So as to emphasize if we want to get all the dream under pervasive computing come to real, guaranteeing all levels of privacy and privacy related issue must be prior and mandatory.

The most profound characteristics of pervasive computing that pose serious threat on privacy summarized as follows [4][7][13]:

- Pervasive computing components will be practically everywhere and affect nearly every aspect of our life style.
- Pervasive computing components will be invisible and potentially act transparently for many users.
- The enhancement of storage capabilities will make easier the access and process of personal data.
- The enhancement of sensory equipment, combined with the advances in their storage capabilities, will make feasible to perceive memory prosthesis or amplifiers, which can continuously and unobtrusively record every action, utterance, and movement of individuals and their and our surroundings.
- The minimization of sensors, as well as the advances in data mining technologies, will increase the amount and types of personal data that are invisibly captured and analyzed.
- The communication of the objects in pervasive computing will usually take place by their own initiation, in a way that might disclose personal data to other objects / users, so as to accomplish their intended purpose.

One of the basic issues while trying to address privacy is to understand what kind and level of privacy is required, since it is more subjective enough from person to person, person to service, service to service and the likes. As a result, developers of context-aware applications are tackled

with a tough challenge though needs powerful privacy controls that will maintain and buy users' trust and adequate enough to be implement for all circumstances [15].

1.1.4. Multitier Privacy Preference Selection

This is a multi-level, layered model configured for every singleton centered around their aura once engaged with this trust-based privacy preference system. The multi-tiered aura is structured hierarchically: personal, social, and company levels, each based on the trust a user has naturally established through their relationships. The personal aura where a singleton's labeled and assigned ubiquitous device for private use. The social aura (second layer) includes natural relations such as family, friends and other intimate groups. And the third layer, the beyond, represent the sphere where a singleton actively works and engages socially with various external entities.

All companies, general public service providers, or organizations that have direct or indirect affiliations with a singleton will be placed and communicate at the third-party layer. Once such layering configurations are established, preference selection must also be set to define the necessary level of trust-based privacy preferences. These privacy preferences will be constructed based on either the possible level of reputation (gathered and calculated from request-response values) or the defined aura set for every suspicious or unknown service request.

1.2. Statement of the Problem

Security challenges including privacy protection, access control, secure communication, and data storage have become critical concerns in IoT environments [2], particularly in pervasive computing systems where ubiquitous resource access necessitates context-aware access control models capable of both dynamically adapting to environmental changes and isolating malicious access attempts. These models must address significant variations in users' privacy expectations across different social contexts [16], requiring flexible rule systems to govern perceptual context and privacy preferences as users' desired control levels fluctuate between environments.

To further support the problem of the matter the following sample scenario on fig.1.1 stormed and presented an assumption of partial or wholly pervasive settings. Saba, who works for Andualem at a certain company, is a field representative, a job role involving offsite meetings with clients.

To keep an overview of his field representatives, Andualem integrates a location sharing feature into the organization cars and phones. Andualem's access to Saba's location should depend on her context. While driving to a client he may access her destination and her estimated arrival of time, according to company policies. However, he may not access such information after work hours. Saba, who also has countless friends, few of which are close and trustable, gets to decide who should have access to her private data on the web like to her everyday tweets, blogs…and so on. Saba, who is very sociable and a great humanitarian she is part of different clubs (the book club, chairperson of the "edir" and a volunteer to the Red Cross to say the list) needs to enforce a schedule or time-based access of her needed private data from these different parties. Like for example, if the red cross is planning on doing some work and is in need of few healthy volunteers which would involve accessing and analyzing their medical records needs to first by pass Saba knowledge and to what extent they would be granted access to, depending on her trust on Red Cross, the edir members her delegate on the other hand may be granted access to her where about if she is a bit late on a meeting, they may also be granted access to her occasional tweets or notifications on when the next meeting is going to be. Saba, who also has access to her former school system (a system that publishes the achievements of its alumni to motivate its current students. Abraham who is Saba's landlord, who by the way never missed a day when collecting a rent occasionally, missed Saba when she was out on a field work, though very risky Saba had no choice but to grant him access to her rent account she opened up at commercial bank. She should also be able to enforce her privacy rules through third parties like in here, the banking system, so he will not access the account again and by regenerating the key and notifying her later on.

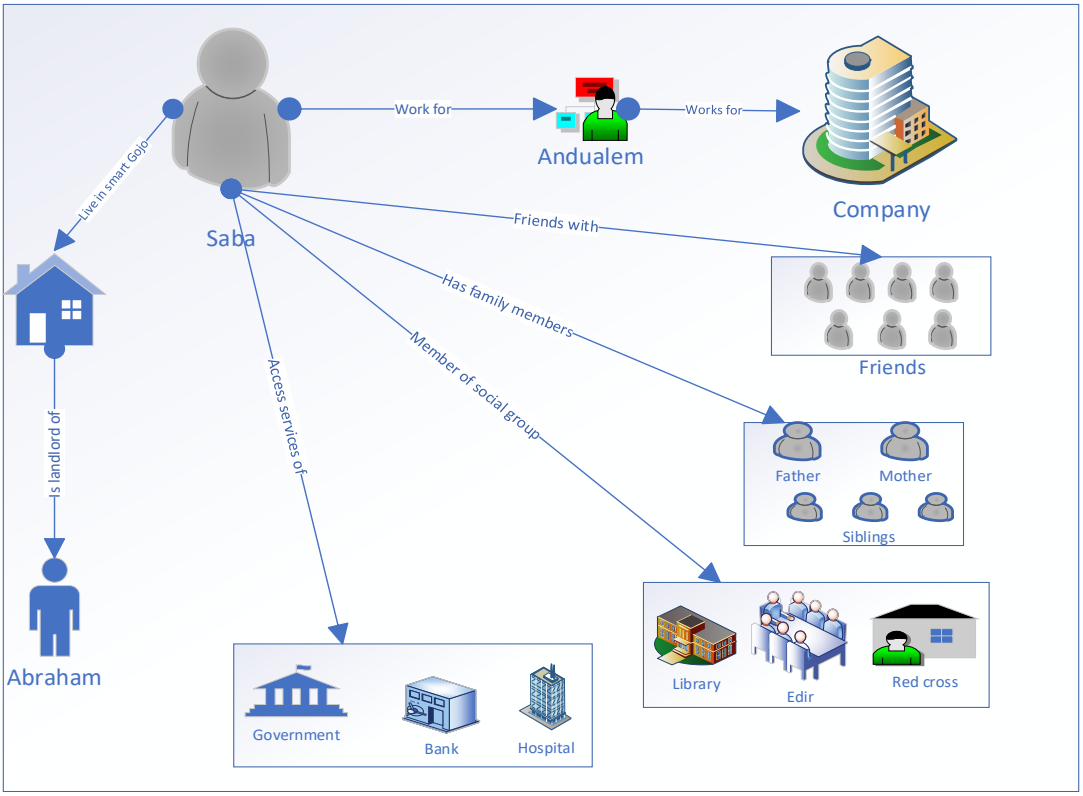

Fig. 1.1: Saba inside a ubiquitous environment

Fundamentally when a singleton like 'Saba' found herself under such busy and highly engaged context aware pervasive environment, how can she address issues of trust on her personal identifiable information's in more generic self-aware privacy control from malicious and spoofing treats. Specifically, whenever there is a request (short message for crowd funding, survey or public services etc.) of service from a certain agents or node, what will be security mechanism either to deny or authorize such sensitive and classified information for numerous, heterogeneous and unknown call even though she needs the service by her own good will's.

The question is while controlling and managing all her numerous requests of service why not she can use her trusted group as an opportunity in order to identify any malicious requests of service by consulting from the group she already develop trust.

Therefore, since privacy with the absence of generic layout would be a challenge to manage and control malicious requests in a context-aware pervasive environment, this research work proposes a generic multitier privacy model based on preference selection to improve the privacy of personal identifiable information (PII).

This study, A Generic Multitier Privacy Model for Preference Selection (GM-PMPS) in a Pervasive Environment, aims to answer: (1) How can a multi-tiered (personal/social/beyond), context-aware privacy framework balance usability and security in pervasive computing? (2) What mechanisms enable dynamic trust evaluation (e.g., "aura" scoring) for IoT access control while adapting to evolving user contexts? and (3) What architectural solutions can address IoT security challenges (data, communication, malicious access) within a layered trust-based system?

1.3. Objective of the Study

1.3.1. General Objective

This research aims to propose a Generic Multitier Aura Framework that transcends domain-specific constraints in pervasive computing environments, enabling user-centric privacy preference selection through a dynamic, condition-based trust model. The model leverages reputation metrics derived from a singleton's defined social circles (personal, social, and institutional tiers) to autonomously adapt access control and data protection policies.

1.3.2. Specific Objectives

This study aims to achieve the following specific objectives:

1. Design and configure a multitier aura framework by stratifying trust boundaries (personal, social, and institutional layers) to enforce context-aware privacy preferences.
2. Establish a request-reputation archive to log and quantify interaction histories, enabling dynamic trust scoring.
3. Define preference selection criteria for adaptive privacy controls based on user-specified conditions and reputational thresholds.
4. Generate and analyze sample request-reputation transactions to validate the model’s responsiveness to evolving trust contexts.
5. Develop a functional prototype demonstrating the framework’s viability in real-world pervasive computing scenarios.

1.4. Methodology

The intention and approach of this project is to create and configure a multitier aura, which is a software architecture that distributes the functionality of an application among different tiers. The project also involves setting up a request reputation archive, which stores information about the requests and their reputations, such as the source, destination, priority, and feedback. The project also sets the proper preference selection criteria, which are the rules that determine how the requests are processed and allocated by the aura. The project also populates sample request reputation transactions, which are the interactions between the requests and the aura, such as sending, receiving, evaluating, and updating. Finally, the project populates a prototype, which is a working model of the aura that demonstrates its functionality and performance.

In order to address the methodology mentioned above, this research uses tools like MS Visio for design diagrams and NetBeans IDE 8.02 for prototype development using the Java language.

1.5. Scope and Limitation of the Study

The major deliverable of this work, however, is developing a model that can solve issues on a more generic end-user level for Pervasive Computing Environments (PCEs) as a whole, irrespective of domain specifics. This proposed model concentrates only on a software-level context system that works for ubiquitous devices. The work extends only up to developing a prototype showcase, which will not involve deployment.

1.6. Significance of the Study

The model itself will be highly useful for addressing privacy issues in ubiquitous environments, as it provides generic yet flexible guidelines that can be customized to solve specific contextual privacy problems for end-users. While the full realization of this envisioned environment could significantly simplify the development of rule-based contextual services, this brainstorming model specifically applies to scenarios requiring personal-level privacy preference setups. Its primary purpose is to protect personally identifiable information (PII) from malicious attacks using manageable techniques, enabling general users to safeguard their data and location with minimal effort.

This model offers researchers a novel framework to study adaptive privacy mechanisms in pervasive computing, providing a testable foundation for developing context-aware, user-centric security solutions beyond domain-specific limitations.

1.7. Organization of the Report

This thesis is organized into six chapters. **Chapter One** introduces the study by providing an overview of [briefly state the focus, e.g., "privacy challenges in pervasive computing"]. **Chapter Two** presents a review of the literature and related works. **Chapter Three** provides a detailed discussion of the proposed model, **GM-PMPS** (Generic Multitier Privacy Model for Preference Selection). **Chapter Four** covers prototype implementation and evaluation scenarios. Finally, **Chapter Five** concludes the study and outlines future work directions.

Chapter Two

2. Review of Literature and Related Works

2.1.Overview

With the introduction of pervasive computing, the world of computing is embedded and distributed in every object that communicates with each other via a wireless connection. The computer we now refer to as a "computer" is placed in the background, barely visible and intrusive, while supporting the dynamic connectivity of the pervasive environment. And this will be true through the three pilar points that consists of user agents, devices embedded to the environment and the internet.

To this very nature of the service, Once the idea of pervasive computing comes into play, a number of research works have been conducted largely on privacy and security. Security and privacy by its behavior has got its own challenges in any system and this is due to the fact that it needs an absolute shield of its entire loop hole. More over security and privacy is became even more challenging for a system like that exist everywhere and at any given interval of time, which is also services are in need to be context aware and users need privacy for their classified and personal identifiable information's. Thus, security is continuously a fundamental issue especially in ubiquitous and pervasive computing environments because these networks differ from traditional wired networks and it has special characteristics such as shared resources, node mobility, short transmission range, absence of central control, dynamic topology and sometimes scalability of this network needs to be handled. Though resolving privacy and security under pervasive computing environment is undoubtable that one of most challenging sectors.

As a result, there are a number of scientific researches endeavored and proposed in order to realize and address security and privacy related matters under pervasive computing environment. This section will go under researches that are mainly concern on trust related security-based papers and present a reviewed report with a closing summary.

2.2.Literature Review

Mariappan and Dhana Balachandran [18] proposed a policy aware privacy enhancement model using dynamic trust and security management techniques. By participate different entities' policy

to achieve an enhanced privacy for on demand request. While using this method there will be high risk of attack like DDoS. This paper targets dynamic trust management framework using two routing techniques namely reliable single and multipath algorithm. The finding of this work identified reliability in both techniques but which may not hold good in reality due to duplicate are not forwarded.

Boukerche, A. and Ren, Y., [19] projected security system by reputation- based trust system that can track the behavior of node and develop trust model. It presents the concept of a novel trust and formulates the theory of trust and community model that can compute trust value of a node. The concept of this trust management involves developing a trust model, assigning credentials to nodes, updating private keys, managing the trust value of each node, and making appropriate decisions about nodes' access rights. Accordingly, this reputation-based trust system can track the behavior of nodes and thereby proceed by rewarding well-behaved nodes and punishing misbehaving ones in order to address the required level of security. While presenting the concept of trust and formulate the theory of trust this research use trust computation and management system the trust value is computed generally based on the linear function and introduces the concept of community node that is a central node this is way too far to actualize under distributed pervasive computing environments.

Stelios D. et al., [1] introduce a generic Privacy Enhancing Model called PEM-PC through a holistic way by incorporating social as well as technical issues. This generic analysis concern with the evaluation of the contextual information takes place and the threat management module by users' device. The primary concern of this research is all about identifying what type of data is usually needed to be shared and for what purpose. Eventually, the issue may be raised data privacy itself may depend on user preference it can't be generic and also there is still a trait from any recognizable malicious third parties that might collect data.

Latif, M.A. et al., [20] proposes a framework called "RESTful URIs" on Smart Home Web of Objects Privacy framework to ensure the personal identifiable information of the users remain protected while releasing sensitive information in the smart home pervasive computing environment. It mainly introduces the Privacy Controller to collect the user PIIs data with other sensory data, the user privacy preferences, and consents about releasing it through a web interface. A Smart Home Web of Object Privacy Processor is under control through user anonymization and

data encryption using privacy controller and privacy processor framework. This Representational State Transfer framework is more appropriate for resource-constrained and ad-hoc environments except being domain specific and it may need to be semantic ontology-based model for privacy protection in a smart home environment.

Cornwell, J.et al., [21] propose a novel mechanism for managing security and privacy in pervasive computing environments, through an application including a contextual instant messenger, a people finder application and phone-based application for access control. This help end-user to manage their security and privacy with simple user interfaces and visualizations for specifying and understanding policies, but it is will be challenged when it faces scalable. A tradeoff also exists between the frequency and timing of user prompts, and the tolerance users have for the system making incorrect decisions.

StephenI.R. et al.; [22] addresses key performance issues, challenges and techniques for privacy control in context-aware web services. While context-aware systems and applications face security threats similar to other distributed and mobile applications, privacy and security aspects are more prominent due do the sensitive nature of context information.

Gaud, N.et al., [23] proposed architecture for context-aware web services based on privacy preferences. This paper aims at contributing privacy management layer to the context-aware web service architecture. The purpose of privacy management layer is to encourage the concept of privacy awareness in this class of services. The author described architecture for privacy in context targeting the user privacy preferences to discover the most secure and flexible web services. The author used the information category chart about user's information for privacy policy and also used sensitive level of the information category according to user convenience. In this paper, with the increase in adoption of context-aware web services developing privacy policies become more and more important as it simplifies the possibility of applying user's privacy preferences.

Yau, P.W. and Tomlinson, A., [24] proposed privacy in a context-aware according to social networking based on recommendation system for enterprise. This paper outlines hierarchical privacy architecture, because users are willing to share private information. So, the protection of private information is needed. The author aimed at developing instant knowledge privacy architecture to provide privacy services to both enterprise and its users. In this paper the author used IK model that is instant knowledge model to developing privacy in context-aware system.

Although privacy is a social construction, modern technology has changed the landscape of how privacy needs to be controlled. Thus, there is a duality between technical solutions and the social structures in which those solutions operate, with the help of model of the IK system a proposed technical privacy requirement for the model and the social implications motivating these requirements.

Dehghantanha, A. et al., [25] proposed privacy evaluation model called User-centered Privacy Evaluation Model (UPEM)for pervasive computing environments. The researcher aimed to handle privacy evaluation using three major criteria: user control over private information, expressiveness of privacy policies and Unobtrusiveness of privacy mechanisms. The works that have been done in this area can generally be categorized in two, as to protecting the privacy in ubiquitous environment. One is trying to solve privacy issues by modelling information-centric frameworks and the other is trying to solve privacy related issues by modelling a user-centric framework. The two try to approach the issues of privacy from different ends prioritizing information context over user context and vice versa. Engulfing the use of either a policy or trust-based themes.

Schaub, F.et al., [26] addresses the issues related to privacy in ubiquitous environments by deriving a generic privacy context model as a context abstraction for arbitrary scenarios, basically by identifying entities and classifying them into territorial bases as observers and disturbers. However, lacks the integration of trust in the model. It has the potential to reduce the complexity of adaptive privacy systems by pre-filtering relevant privacy components. As a key contribution, the model takes information as well as physical and territorial aspects into account. However, does not incorporate trust in the model, given the importance and the generic nature of the work.

Chakraborty, S. et al., [27] proposed inference-based model, such that those indicating the user's behavior cannot be drawn. Focuses on the more general problem of choosing what data to share, in such a way that certain kinds of inferences i.e., those indicating the user's sensitive behavior cannot be drawn. It is strictly policy based (defines inferences in two types as blacklist and white list) which is so rigid and wouldn't cope with the dynamicity of contexts, and there is no indication on what interval the list will be updated and no such method is described that is used to describe the information inside either of the list.

Ackerman, M.S. et al., [28] presents a super-ego, a crowd sourcing framework for privacy management of location information in ubiquitous environment. The work studies how crowd

sourcing can be used to predict the user's privacy preferences for different location on the basis of the general user population. The collective intelligence of the crowd is harnessed to solve difficult problems that cannot be solved directly using computation or human effort. By just following two steps afterwards the collection of immense knowledge, one being predicting the user's privacy preferences and making privacy management decision. However, while widespread adoption of super-ego can eventually lead to the creation of knowledge base it is limited to requiring knowledge about location disclosure from the general population.

Almutairi, S.et al., [9] propose review on security frameworks in context aware system in order to provide reliable security to context aware systems and applications. Upon this issue the paper checks the requirement and design consideration on computing context, user context, physical and time context. The work addresses different framework in context aware system security and suggests Kerberos frameworks on authentication and access control and privacy as a compatible security requirement. But still some further work has to be done in order to address total privacy and un-traceability of users, since both of the frameworks relies on user related data which includes fingerprint, voice and face recognition.

Pingley, A.et al., [29] presents a context-aware privacy preserving model for location-based services with integrated protection for data privacy and communication anonymity by using third party anonymizer. The work addresses two challenging issues: protection of user's location privacy from both location data and network communication perspectives. However, the accuracy highly depends on the number of surrounding entities, that has the potential of deducing the exact location if that number appears to be very small.

Lederer, S. et al., [30] this research work introduces a conceptualize framework for designer and administrators to protect privacy in ubiquitous computing device through a metaphor privacy model. The researcher develops a situational faces metaphor where individual can manage privacy implication of a given situation through intuitive and adequate notice of user understanding. In this research model users are offered to select his or her preferred face, which is an abstraction of a permutation of privacy preferences applicable to the situation the ubicomp system and codify the user's conditional consent to disclose certain personal information in exchange for ubicomp services. Nevertheless, the situational faces metaphor gets challenged, since users are very hesitant to configure a large set of descriptive preferences and parameters.

Amini, M. and Zokaei, S.;[31] Due to users are being mobile and numerous in its very natures this paper proposes a new context-aware access control model for pervasive computing environments. Hence a role-based access control model is proposed and assign roles to users dynamically, based on the long-term context information and short-term context information of user's environment that can tune active role's permissions accordingly. This architecture use domain authority and session agent that address the context-based information with integrated level of constraints which can maintains all user's role. Meanwhile the likely challenge of this role-based model is, that of reloading context for each event, it will be time taking and inefficient especially when things are at large scale.

Schaub, F. et al, [32] propose a higher-level context model that abstracts from low level details and contains features facilitates identification of privacy relevant context changes and analysis of their potential privacy implications in order to decide when to dynamically adapt privacy mechanisms and how. The context model abstracted privacy relevant context information to the user and model to reflect a user activity as essential. The system will adapt to individual users by learning their privacy preferences over time from explicit privacy decisions and implicit reactions to autonomous reconfiguration of privacy mechanisms. A major challenge in the instantiation of the proposed model is the detection of physically and virtually present entities and channels.

Boukerche, A. and Ren, Y.,[33] propose a novel trust-based security management system called Trust computation and management systems. Its managed nodes dynamically, and the node activities are efficiently evaluated in a distributed manner. Based on the trust matric measured a malicious node can be detected and communicated within the community in order to penalized and decreases its trust level.

Sharma, S.et al.,[34] propose a secure reputation-based architecture for MANET network and routing model forming backbone node to maintain neighbor table, reputation level table and legitimacy value table, which are used to kept information about all the nodes. The proposed scheme will attempt to create a route that does not go through a node whose replied information is wrong and PPN term is not fully divisible and reputation value of that node crosses the threshold value. Based on node level or reputation value the system will call either removal of malicious node to maintain the MANET routing security level or repeat the process to further data transmission.

Kapitsaki, G.M., [35] propose a Context-awareness offers user's services; in this paper the reflection of user privacy preferences in the provision of context-aware web services is addressed. The author introduces consumer privacy language is proposed with an adaptation mechanism for SOAP messages. The author used consumer privacy preferences for comparing personal context with environment context and used privacy enforcer architecture to developed privacy preferences in context-aware web services.

Sievers, M. et al., [36] propose and construct state emission and transition probabilities by observing agent inputs and outputs. Factors like internal faults, unintentional user errors, malicious actions, and unexpected environmental conditions and stressing usage may create situations in which one or more agents become untrustworthy. Systems may become unstable when consistent understand of health and operation is not achievable. And proposed a means that accounts for the influence that reputation plays in establishing updated belief states and identified the need for adaptive mechanisms that can gradually adjust reputation and emission probabilities. Those probabilities are dynamically changed in response to changes in reputation which impacts agent actions.

2.3. Summary of Related Works

As demonstrated in the researches above, numerous studies have proposed, implemented, and widely utilized trust-based security frameworks for pervasive environments. These studies address domain-specific applications such as smart home services [20], context-aware web services [34], context-aware social networks [10], and MANET routing [35], among others. A recurring theme across these contributions is their emphasis on security challenges in context-aware ubiquitous networks.

However, a critical gap persists: existing solutions are not generic and lack end-user-managed adaptation mechanisms to (1) compensate for individual weaknesses and (2) preserve anonymity during interactions in pervasive environments. Crucially, local trust exchange—the foundation for reputation-building and safe societal environments—remains underexplored in these rigid, domain-confined approaches.

Chapter Three

3. Proposed Model

3.1. Overview

In this chapter, the proposed privacy preference model, a generic multitier privacy model for preference selection in a pervasive environment (GM-PMPS), is presented and briefly explained with regard to the specific privacy requirements in pervasive computing. The functionality of the propped model is presented into two categories, namely a generic multi-tier and privacy model preference selection based on trust which is built on reputation as the main parameter of this work. Accordingly, this chapter first introduces the architecture of the proposed model and then briefly discusses trust and reputation in the context of the GM-PMPS model. Finally, the design procedure is presented through the configuration method and the pseudo-code of the proposed model

3.2. Structure of GM-PMPS Model

As indicated above, this research has two broad foundations: namely, a generic multitier architecture and a privacy model preference selection that depend mainly on a set of trust values developed through reputations.

The generic multi-tier architecture defines different auras arranged as personal, social, and third-party layers within pervasive computing environments. This multilevel model classifies privacy requirements based on aura levels. The personal aura, serving as the core of the architecture, encompasses all ubiquitous devices belonging to an individual. The second tier, called the social aura, projects both direct and indirect connections to personal auras. This social aura emerges from points where personal auras begin associating, governed by established trust and reputation metrics. The third tier, the third-party aura, represents organizational entities that form independent interaction circles while maintaining connectivity with personal and social auras.

The Preference Selection Privacy Model builds upon the aforementioned architecture, defining individualized privacy criteria and interaction conditions for each aura tier. This model establishes adaptable preference-selection mechanisms that activate when unknown interventions or requests occur, ruled by condition-based trust metrics derived from reputation systems.

Key components include:

- Conditioned-Based Trust: developed through accumulated reputation scores from historical interactions between parties within each aura
- Dynamic Trus Adjustment: positive/negative reputation outcomes from prior engagements automatically modify trust levels for future preference selections
- Automated Implementation: The system technically embeds these trust parameters to autonomously regulate privacy preferences

The model's core innovation lies in its reputation-driven, self-adjusting mechanism for privacy management across all aura tiers (personal, social and third-party).

In most context-aware systems, three primary operations persist throughout the service lifecycle in pervasive environments [3]: (1) context data collection, (2) data analysis, and (3) service provision. A layered architectural approach proves optimal for enhancing mobility, modularity, interoperability, compatibility, and flexibility in such systems [12]. This pervasive computing framework functions as a conceptual model that remains adaptable to accommodate unforeseen tasks or entities that may emerge during implementation.

To better understand and visualize the proposed Generic Multi-tier Privacy Model for Preference Selection (GM-PMPS) in pervasive environments, refer to the diagram in Fig 3.1.

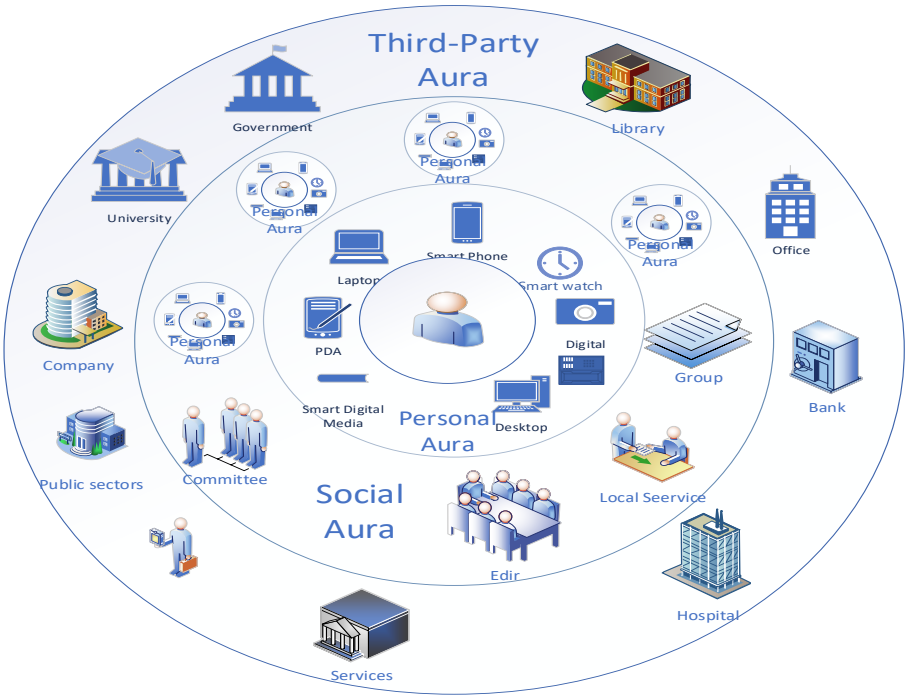

Fig. 3.1: Multi-tier aura layer visualization

The model centers on an individual, whose personal aura comprises their smart devices and forms the foundational layer for privacy preference management. The second layer, the social aura, encompasses connections with friends, groups, and shared activities. The outermost layer consists of third-party entities, primarily service providers, governed by the privacy preference selection model. This structure directly mirrors real-world social dynamics - when encountering unknown service requests (typically from outside one's immediate circle), individuals naturally seek social verification before engagement, mirroring how trust and reputation develop gradually in physical interactions.

3.3. Trust and Reputations Inside GM-PMPS Model

The adoption of pervasive computing infrastructures introduces significant privacy and data protection challenges [5]. Conventional security mechanisms prove inadequate for such environments, as they cannot rely on (1) a shared infrastructure to enforce behavioral norms, nor (2) universally accepted standards. Unlike traditional systems, pervasive computing lacks a central authority to establish and enforce rules, rendering conventional governance models ineffective [1].

Faced with selecting reliable security methods, users increasingly turn to peer networks and trusted sources within their environment - leveraging pre-established service reputations as decision-

making criteria. This research consequently focuses on formalizing these real-world trust and reputation mechanisms into computational frameworks. The ultimate objective is to develop a secure, generic multi-tier pervasive computing system grounded in preference-based selection.

Trust-based security mechanisms have emerged as a solution and significantly expand the scope of traditional security models. Trust enables people to accept risk and deal with uncertainty. Trust in the literal sense of the word is more difficult to achieve in such a complex and dynamic space we live in, and is also subjective and dependent on the consumer's perspective. However, online environments such as the Internet, search engines, peer-to-peer networks and new applications built on highly complex social networks present a number of challenges in the interpretation and use of online trust and reputation systems [19].

Trust is a relationship between two entities in which one entity believes, expects and accepts that the other trustworthy entity will act favorably or intends to do so [30]. While trust and trust management are bestowed in one way or another, it is accompanied by a reputation that endures over time. The beliefs or opinions generally held about someone or something determine the level of trust we develop. On the other hand, an entity's reputation has been defined as an expectation of its progressive behavior based on observations or information from other entities about the entity's past behavior in a particular context at a particular time [3]. To keep up with such a computing world, we examine and utilize trust and reputation to achieve a higher level of security.

Even though the formulation of the theory of trust has a more general meaning for the community, the concept of trust is also used in pervasive and ubiquitous computing environments and is widely applied nowadays. Trust management for pervasive computing environments in terms of security policy is responsible for assigning credentials to entities, delegating trust to third parties, and deciding users' access rights.

Nowadays, we see smartphones and numerous digital devices everywhere that can sense and react to contextual data thanks to their numerous sensors and high processing power. The fact that such devices can understand the real world and provide automatic services is one reason for the development of context-aware mobile applications that proactively respond to the user's environment [30]. However, in order to freely use a context-aware environment, we need to be sure that such a system and environment are trustworthy and secure when we delegate and access a certain service. Even though the context- aware environment changes rapidly and includes more

details such as nearby people, devices, lighting, noise levels, network availability, temperature, humidity, light sensors, accelerometers and more, it still needs to protect privacy and security.

To date, several privacy enhancing technologies have been proposed, implemented and extensively used, mainly for the Internet/network paradigm. However, as various privacy threats emerge in pervasive environments, there is a high need and requirement to close this security breach in everyday services.

Contemporary privacy protection is legally codified through specific laws, regulations, and directives across numerous jurisdictions. Within pervasive computing environments, adherence to fundamental privacy principles becomes imperative for maintaining fair information practices. This research's proposed model aligns with the framework established at the 4th International Conference on Ubiquitous Computing regarding Privacy Awareness Systems for Ubiquitous Computing Environments. These principles serve as essential guidelines for developers implementing pervasive computing applications.

- Notice: Users must be explicitly informed about personal data collection processes.
- Choice and Consent: Users retain absolute control over whether their personal data is collected or processed.
- Proximity and locality: The collection of data from a user's device should only occur when the user is present (proximity). Processing and access to this data should only take place in the space they were collected (locality).
- Anonymity: Whenever the identity of the user is not required or the user does not consent, anonymity services should be provided.
- Security: Implement robust protection mechanism ensuring data integrity, confidentiality and protection against unauthorized access
- Access and resources: Access to the user's data should be restricted to authorized entities only. There should be regulatory means for the protection of a user from parties who do not adhere to this regulatory framework.

This paper proposes a simplified trust-reputation model within the GM-PMPS framework, establishing formal relationships between (1) attributive trust and (2) problem-solving capabilities in corporate reputation systems. The model advocates for a comprehensive privacy paradigm integrating three critical dimensions -- social norms, regulatory frameworks, and technological

safeguards - to ensure robust end-user privacy protection through trust and reputation in pervasive computing environments.

3.4. Design Procedure for GM-PMPS Model

The primary objective of this Generic Multi-tier Privacy Model for Preference Selection (GM-PMPS) in a pervasive environment is to design and develop a model that creates context-aware trust through reputations. It is a model that is able to perceive changes in the user's environment, a process that is able to respond with and without user intervention and a process that is able to offer different behaviors to meet diverse user needs. While context-aware systems can be implemented at both hardware and software levels, this research specifically focuses on high-level (software-layer) context systems, as established in the research objective. Although the software layer integrates multiple data sources and computational capabilities, the model's core operation involves trust-value computation through reputation metrics across defined multi-tier auras. Each aura tier incorporates a dedicated trust module that processes collected reputation values to determine trust levels.

Trust and reputation are therefore key elements in the development and implementation of these multi-tier systems. Basically, reputation is used to quantify the level of trust one can place in a trustworthy party based on previous experience interacting with the agent in question. In the implementation of this trust and reputation model, a decentralized or distributed approach is followed, where agents must keep their own interaction references with the aura and estimate trust based on the multi-level aura created by the singleton at the center.

Hence, in order to address the preference selection of this proposed work, condition-based trust is implemented by witness-based reputation and interaction-based reputation based on the established level of aura. Witness-based reputation depends on the feedback from the friends or society, i.e., if the social or the company level aura confirm or guarantee the agent or service is trustee for responding to the request and the beneficiary has either approved or rejected the service. Witness reputation will participate by giving, tracking and evaluating referrals. The second type of distributed reputation, delivered under reputation by interaction, depends directly on the record of previous interactions. The singleton in the middle then guarantees that the trust level of the service is decent or not to continue the interactions and allow service requests.

To realize this distributed reputation model in the context of multi-tier preference selection, each agent can evaluate the reputation of others and/or its own dataset, since there is no central repository shared by all. For example, when there is an unknown or suspicious request for services, the node refers to its aura by sending a broadcast message to all and calculates the weighted average based on the response value of the request before making a decision. Each aura does this to obtain the trust value for the witness reputation in addition to the interaction trust value. Then the direct trust is calculated as a weighted average of all ratings together with the rating time. Since trust is dynamic by nature, what behaves today is no guarantee for tomorrow. A user may cheat on some interactions after receiving a high reputation score [20]. A direct trust is calculated using the weighted average of all ratings. The weighted value is higher if it is a current value, as today's trust value is more accepted than yesterday's, even if the rating sets are the same [29].

Although GM-PMPS is a decentralized model based on reputation conditions, which is much more suitable and feasible in practice, it has its own potential in terms of privacy and security under the conditions of pervasive computing.

The design of this distributed trust under witness reputation is illustrated in Figure 3.2. Assuming node ‘A’ wants to link a service to node ‘B’, node ‘A’ will ask node ‘C’ if node ‘B' is trustworthy or not. Based on the response to the request, node ‘A’ can then proceed automatically or allow the user to intervene manually or block the service altogether.

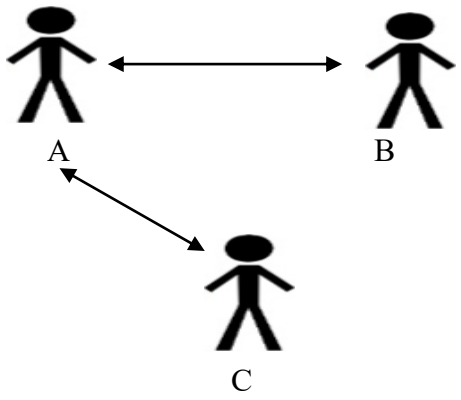

Fig.3.2: Trust through witness reputation

Interaction trust arises when node A desires a service from node 'B'. Node 'A' judges from personal experience whether node 'B' is trustworthy and offers or rejects the service. This trust and the reputation between the nodes are based on the value of the archive entries over the time of the previous interaction (see Figure 3.3).

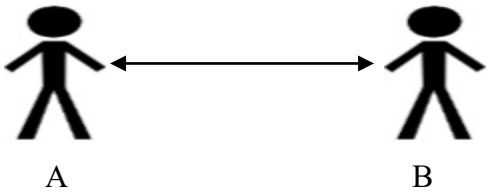

Fig.3.3: Trust through interaction

Reputation is mainly used to quantify the level of trust generated by a certain type of interaction. In order to practice the above two distributed trust reputations and quantify the level of trust, the study proposes the following system model, which is integrated into a multi-tier aura model.

Each mobile node will be configured with GM-PMPS locally and thereby offer accesses to nodes in its defined aura according to their reputation value that can buy a required level of trust that will be set by users' preference selection point. Though, based on the request response values the GM-PMPS calculate a weighted average where response value times by bias number over the total number of responses, (see equation 3.1) and compared with the preference selection set value in order to decide on service request needs either automatic replay, manual intervention or deny request.

$$\text{Weighted average} = \frac{\sum(\text{Response values} * \text{bias number})}{\text{Total number of responses}} * 100 \qquad (3.1)$$

The configuration setting and pseudo code of this privacy model is further elaborated in respective order.

3.4.1. Configurations for GM-PMPS Model

This Trust and Reputations Inside GM-PMPS Model configured according to the design procedure mentioned above as of the following basic arrangements.

- Create the Aura Interfaces
  - ✓ Personal Aura
  - ✓ Social Aura
  - ✓ Third party Aura

- Set and configure node values
  - ✓ Set personal nodes
  - ✓ Set social nodes
  - ✓ Set third party nodes
- Set the possible transactions
  - ✓ Request
  - ✓ Services (location, media)
- Set Archive
  - ✓ Request – Reputations
- Set Evaluation
  - ✓ Preference selection values
- Compute the service trust on weighted average value to be
  - ✓ Automatic reply
  - ✓ Manual intervention
  - ✓ Deny request

3.4.2. Pseudo Code for GM-PMPS Model

Start

Configure node states

{

Personal aura

Social aura

Third-party aura

}

Set preference Selection

{

bias value for personal aura

bias value for social aura

bias value for third-party aura

return (weighted average)

}

```
16.     Set archive {
17.         Update(reputation)
18.     }
19.
20.     Set service type
21.     {
22.         location
23.         media
24.     }
25.
26.     Read possible Service Request (Request ID)
27.     Broadcast Request ID to every node
28.     Receive Request Reputation (0,1)
29.     then buffered to the preference selection
30.     Call preference selection
31.
32.     Process Request Reputation in accordance to node state value
33.     {
34.       If (Response get from personal aura node)
35.           then bias to be 1 and multiply the response number and get reputation response
              value
36.       else if (response from social aura node)
37.           then bias to be 0.9 and multiply by number of response and get reputation
              response value
38.       else (Response from third party aura node)
39.           then bias to be 0.8 and multiply by number of response and get reputation
              response value
40.       Return weighted average (response values*bias figure/total responses) *100
41.     }
```

42. Store reputation

43. Call personal aura weight configuration

44. {

45. If (weighted average value is equal to -1)

46. then no reputation

47. else if (weighted average value is equal or greater than personal aura Auto weight)

48. then allow service to be automatic

49. else if (weighted average value is equal or greater than personal aura manual weight and less than personal aura auto weight)

50. then call manual intervention

51. else

52. block service request

53. }

54. Stop

Chapter Four

4. Prototype Implementation and Evaluation of the GM-PMPS

4.1. Overview

This chapter presents the implementation of proposed prototype of this Generic Multitier Privacy Model for Preference Selection. This model as it is proposed earlier on the design it mainly concern on building a multitier aura and proceed with the possible preference selection of trust-based privacy system. A prototype and a sample scenario with a closing summary carried here accordingly.

4.2. Prototype Implementation

Generally, the proposed prototype implementation of GM-PMPS detailed specification and description are briefed as follows.

- Create and configure the multitier aura interface to implement the GM-PMPS model as of personal, social and third party with defined name and weight range criteria as shown on fig. 4.1.

```
package Configuration;

public interface Aura {
public void setName(String name);
public void setAutoWeight(double value);
public void setManualWeight(double value);
public void setBlockWeight(double value);
public double getAutoWeight();
public double getManualWeight();
public double getBlockWeight();
}
```

Fig. 4.1: Aura interface configuration

- Create sample node configuration for each aura level using aura, device Id, device name and owner as shown on fig. 4.2.

```
package Entities;

import Configuration.Aura;

public class Node {
Aura aura;
long deviceId;
String deviceName;
String owner;

public Node(Aura aura, long deviceId, String deviceName, String owner) {
this.aura = aura;
this.deviceId = deviceId;
this.deviceName = deviceName;
this.owner = owner;
}
```

Fig. 4.2: Node configuration

- The personal aura implementation with that of weight definition for possible privacy preference criteria as shown under fig. 4.3.

```
package Entities;

import Configuration.Aura;
public class PersonalAura implements Aura{
   String name;
   double autoWeight;
   double manualWeight;
   double blockWeight;
}
```

Fig. 4.3: Aura implementation

- Populate sample request for random node using request Id, request source and service (location, media) and store reputations in order to realize the sample prototype here under fig. 4.4.

```
package Transaction;
public class Request {
   long requestId;
   String requestSource;
   int service;
   public Request(long requestId, String requestSource, int service) {
this.requestId = requestId;
this.requestSource = requestSource;
this.service = service;
   }
```

Fig. 4.4: Request Transaction

- Generate a sample reputation to a random node under request reputation archive using the request node, request number and values present under fig 4.5

```
package Archive;
import Entities.Node;
import Transaction.Request;
public class RequestReputation {
   Node node;
   Request request;
   int value;

   public RequestReputation(Node node, Request request, int value) {
this.node = node;
this.request = request;
this.value = value;
   }
```

Fig. 4.5: Request Reputation Archive

- Evaluate the preference selection based on node state bias value and return formulated weighted average as shown under fig. 4.6

```
package Evaluation;
public class PreferenceSelection {
   public double calculateWeightedAverage(Request request,
ArrayList<RequestReputation> reputations){
      System.out.println("REQUEST BEING EVALUATED WITH ID " + request.getRequestId());
      System.out.println("LOGGED REPUTATIONS");

      double totalResponses = 0;
      double responseValues = 0;

for(int i=0;i<reputations.size();i++){
        if(reputations.get(i).getRequest().getRequestId() == request.getRequestId()){
System.out.println(reputations.get(i).toString());

           double bias = 1;
           if(reputations.get(i).getNode().getAura() instanceofSocialAura){
              bias = 0.9;
}else if(reputations.get(i).getNode().getAura() instanceofThirdPartyAura){
              bias = 0.8;
           }
responseValues += reputations.get(i).getValue() * bias;
totalResponses++;
        }
      }
           if(totalResponses==0){
        return -1;
      }
//      System.out.println(totalResponses); weighted average
      return (double)(responseValues/totalResponses)*100;
   }
}
```

Fig. 4.6: Preference selection

Based on the bias level set value for each aura all kind of service request will be broadcasted and evaluated. The final result then be judged either to be automatic replay, manual intervention or deny the request. The prototype of this model further evaluated through a sample scenario on the next section.

4.3. Sample Scenario

The sample scenario for this user-centered privacy preference model implementation considers the following assumptions and presents the findings at the end.

Assumptions on the sample scenario

- Configure list of nodes under
  - Personal aura → 5 nodes
  - Social aura → 150 nodes
  - Third-party aura →250 nodes
- Populate 500 random sample request
- Populate 5000 random sample reputation and stored under archive list
- Set magnitude value of biasness to be 1.0,0.9 and 0.8 for personal, social and third party respectively
- Set the personal aura privacy preference weighted average value as
  - Weighted average >= 50 → for automatic preference selection
  - Weighted average >= 20 → for preference on manual selection
  - Weighted average >= 0 → for block service request

Based on the assumptions above the following sample scenario generate 3 random service requests in order to show all possible options (automatic replay, manual intervention or deny request) on the preference selections using request id and return a calculated value and preference selection decision as follows.

Scenario 1:

LIST OF NODES (from personal, social and third-party)

Saba Kebede - SK_7
Saba Kebede - SK_88
Saba Kebede - SK_34
Saba Kebede - SK_30

Saba Kebede - SK_7
Contact1 - ABC_51
Contact2 - ABC_60
Contact3 - ABC_63
.
.
.
Contact148 - ABC_20
Contact149 - ABC_18
Contact150 - ABC_92
Org1 - XYZ_51
Org2 - XYZ_81
Org3 - XYZ_36
.
.
.
Org248 - XYZ_27
Org249 - XYZ_57
Org250 - XYZ_35

LIST OF REQUESTS

---

0 - REQ_0
1 - REQ_1
2 - REQ_2
3 - REQ_3
.
.
.
497 - REQ_497
498 - REQ_498
499 - REQ_499

LIST OF REPUTATIONS

XYZ - 185_0
XYZ - 199_0
XYZ - 343_0
ABC - 175_0
ABC - 341_0
.
.
.
XYZ - 201_1
XYZ - 129_0
XYZ - 431_1

REQUEST BEING EVALUATED WITH ID 387

LOGGED REPUTATIONS

ABC - 387_0
XYZ - 387_1
ABC - 387_0
ABC - 387_1
ABC - 387_0
XYZ - 387_0
XYZ - 387_0
ABC - 387_0
ABC - 387_1
XYZ - 387_1

CALCULATED VALUE 34.0 Manual/ User intervention
BUILD SUCCESSFUL (total time: 0 seconds)

Scenario 1: Evaluation

Based on node request id **387**

Logged reputations (request response)

- From personal aura response – none
- From social aura (ABC) response – 6 nodes
- From third-party (XYZ) response –4 nodes
- Total number of responses – 10 nodes

Therefore, the weighted average = (((2*0.9) +(2*0.8))/10) *100= 34.0 which needs user interventions based on personal privacy preference stated value assumptions.

Scenario 2:

LIST OF NODES (from personal, social and third-party)

Saba Kebede - SK_73
Saba Kebede - SK_19
Saba Kebede - SK_2
Saba Kebede - SK_13
Saba Kebede - SK_88
Contact1 - ABC_29
Contact2 - ABC_87
Contact3 - ABC_64
.
.
Contact148 - ABC_98
Contact149 - ABC_13

Contact150 - ABC_10
Org1 - XYZ_52
Org2 - XYZ_25
Org3 - XYZ_91
.
.
.
Org249 - XYZ_44
Org250 - XYZ_48

LIST OF REQUESTS

0 - REQ_0
1 - REQ_1
2 - REQ_2
.
.
.
497 - REQ_497
498 - REQ_498
499 - REQ_499

LIST OF REPUTATIONS

ABC - 127_0
XYZ - 84_1
ABC - 116_1
.
.
.
XYZ - 481_1
XYZ - 209_1
ABC - 169_0

REQUEST BEING EVALUATED WITH ID 37
LOGGED REPUTATIONS

ABC - 37_1
ABC - 37_1
ABC - 37_0
ABC - 37_0
XYZ - 37_1
ABC - 37_1
XYZ - 37_1
XYZ - 37_0

CALCULATED VALUE 53.75Auto/ Go ahead
BUILD SUCCESSFUL (total time: 2 seconds)

Scenario 2: Evaluation

Based on node request id **37**

Logged reputations (request response)

- From personal aura response – none
- From social aura (ABC) response – 5 nodes
- From third-party (XYZ) response – 3 nodes
- Total number of responses – 8 nodes

Therefor the weighted average = (((3*0.9) +(2*0.8))/8) *100= 53.75 which is automatic request response based on personal privacy preference stated value assumptions.

Scenario 3:

LIST OF NODES (from personal, social and third-party)

Saba Kebede - SK_80
Saba Kebede - SK_66
Saba Kebede - SK_11
Saba Kebede - SK_26
Saba Kebede - SK_66
Contact1 - ABC_91
Contact2 - ABC_0
Contact3 - ABC_13
.
.
Contact148 - ABC_30
Contact149 - ABC_17
Contact150 - ABC_89
Org1 - XYZ_20
Org2 - XYZ_78
Org3 - XYZ_77
.
.
Org248 - XYZ_93
Org249 - XYZ_87
Org250 - XYZ_59

LIST OF REQUESTS

0 - REQ_0
1 - REQ_1
2 - REQ_2
497 - REQ_497
498 - REQ_498

499 - REQ_499

LIST OF REPUTATIONS

XYZ - 447_1
XYZ - 348_1
XYZ - 390_1
.
.
.
ABC - 171_0
XYZ - 114_0
XYZ - 3_0

REQUEST BEING EVALUATED WITH ID 148
LOGGED REPUTATIONS

XYZ - 148_0
XYZ - 148_0
ABC - 148_0
ABC - 148_0
XYZ - 148_0
ABC - 148_0
ABC - 148_0
XYZ - 148_0
XYZ - 148_0
ABC - 148_0
ABC - 148_0

CALCULATED VALUE 0.0Block/ Deny service
BUILD SUCCESSFUL (total time: 1 second)

Scenario 3: Evaluation

Based on node request id **148**

Logged reputations (request response)

- From personal aura response – none
- From social aura (ABC) response – 6 nodes
- From third-party (XYZ) response – 5 nodes
- Total number of responses – 11 nodes

Therefore, the weighted average = (((0*0.9) +(0*0.8))/11) *100= 0.0 which is deny service request based on personal privacy preference stated value assumptions.

4.4. Discussion of Result

The findings of this generic privacy model, which relies on the reputation results of nodes from different auras, align perfectly with the privacy preference levels set by the personal aura. As observed in the sample scenarios above, the model generates random service requests for each case and calculates a weighted average based on reputation scores. This process determines privacy preferences using logged reputation values and bias figures assigned to each aura node, ultimately deciding whether to automatically authorize, require manual intervention, or deny the service request.

This study advances dynamic privacy adaptation through a reputation-aware system where decisions evolve with real-time contextual inputs from multiple auras (personal, social, and third-party). The incorporation of seated magnitude values for biasness at singleton preference levels enables precise privacy calibration. Empirical validation via scenario-based testing demonstrates how weighted reputation averages and configurable bias thresholds facilitate reliable, context-sensitive decision automation. The proposed user-centered design empowers individuals to control privacy preferences through a flexible, generic multi-tier framework that uniquely accommodates nuanced trade-offs - particularly in pervasive networks where service access may require partial privacy relaxation. Unlike prior rigid approaches, this model maintains adaptability while preserving granular preference selection across diverse operational contexts.

Chapter Five

5. Conclusion and Future Works

5.1.Conclusion

Since Mark Weiser's pioneering vision in the early 1990s, fundamental security challenges - including privacy-preserving access control, secure communication, and data protection - have remained persistent concerns in IoT systems through three decades of evolution [20]. Pervasive networks represent particularly attractive targets for cyber-attacks, making security mechanisms that can detect compromised nodes and preserve evidence of malicious activities essential for successful deployment [2]. As pervasive computing becomes increasingly integrated into daily life, privacy concerns have grown more prominent. Modern users routinely face unknown service requests for sensitive data like location information and personally identifiable information (PII), creating significant privacy preservation challenges.

Trust plays a fundamental role in addressing user privacy concerns within context-aware service platforms [5]. Recognizing its importance, this work focuses intensively on incorporating trust relationships into privacy model preference selection. The proposed approach enables collective decision-making about unknown service requests through reputation references among trusted groups, mirroring real-world trust dynamics while operating in pervasive environments.

The GM-PMPS model implements this vision by establishing end-user privacy preferences through organic trust development - replicating how individuals naturally consult their trusted circles before engaging with unknown services in daily life. This research strives to bridge the gap between real-world trust behaviors and digital privacy management by developing a reputation-based framework for PII protection. The condition-based trust model, supported by empirical evidence, demonstrates how reputation mechanisms can effectively safeguard user PII in pervasive systems.

While offering significant advantages for user-centric privacy protection, the GM-PMPS model presents limitations requiring attention. Its reputation-based foundation introduces potential vulnerabilities, particularly regarding scalability across heterogeneous environments. The model must also balance robust privacy protections with maintaining service utility, as strict preference

settings may impact functionality. Furthermore, the cold-start problem poses adoption barriers for new users lacking established reputations. Addressing these challenges through future research will be crucial for advancing the model's practical implementation.

This generic privacy framework provides a viable solution for end-user-centered privacy management in pervasive environments, particularly when dealing with sensitive PII. By grounding digital trust mechanisms in natural human behaviors, the model offers a promising path forward for privacy preservation in increasingly connected world.

5.2. Future Works

Developing architectures to address the aforementioned security challenges in IoT environments remains a non-trivial undertaking [2]. An effective IoT architecture must not only resolve existing security concerns but also account for new challenges introduced by deployment across Software-Defined Networks (SDNs) and cloud infrastructure [2]. While the current privacy model presents a viable solution, its capabilities could be expanded through several promising research directions:

1. Ontology-Based Context-Aware Service Integration
    - ✓ Implement intelligent systems capable of learning neighboring node behaviors through multi-dimensional context analysis, including:
        - Temporal patterns (time-based interactions)
        - Spatial relationships (nearby people/devices)
        - Environmental factors (noise levels, network availability)
        - Social context (situational awareness)
    - ✓ This would enable adaptive privacy policies that respond to dynamic environmental conditions.
2. Byzantine Fault Tolerance Enhancement
    - ✓ Develop robust verification mechanisms to:
        - Detect and mitigate Byzantine faults during aura request/response cycles
        - Ensure consensus among agent nodes
        - Maintain minimum operational node thresholds for reliable decision-making

- ✓ Potential approaches could combine cryptographic proofs with reputation-based validation.

3. Bias Analysis in Personal Preference Selection
   - ✓ Investigate service scenarios to:
     - Quantify and mitigate algorithmic biases in privacy preference settings
     - Evaluate how personalization parameters affect decision outcomes
     - Develop fairness metrics for context-aware privacy models
   - ✓ This research could leverage statistical analysis of user behavior patterns.

These extensions would significantly enhance the model's applicability while addressing critical gaps in current pervasive computing security paradigms. Future implementations should particularly focus on the intersection of these three dimensions to create comprehensive privacy-preserving ecosystems.

References

[1] Stelios D, John T. and Dimitris G.,2016, A Generic Privacy Enhancing Technology for Pervasive Computing Environments. Information Security and Infrastructure Protection Research Group Dept. of Informatics, Athens University of Economics and Business, Greece. IS THIS ARTICLE OR MSC THESIS?

[2] Conti, M., Dehghantanha, A., Franke, K. and Watson, S., 2018. Internet of Things security and forensics: Challenges and opportunities. IS THIS ARTICLE OR MSC THESIS?

[3] Kalpana Shankar, Kay H. Connelly, Ethics and Pervasive Technologies School of Informatics and Computing, IS THIS ARTICLE OR MSC THESIS?

[4] Weiser M., "The computer for the 21st Century", Scientific American, Vol. 265, no. 3, pp. 94-104, September 1991.

[5] Philip Robinson Privacy, Security and Trust within the Context of Pervasive Computing, University of Karlsruhe, Germany, IS THIS ARTICLE OR MSC THESIS?

[6] AUTHOR NAME, National Institute of Standards and Technologies, Proc. of the IT Conference on Pervasive Computing, 2015

[7] C. Drost, "Privacy in Context-Aware systems," JOURNAL NAME, 2018.

[8] Musumba GW, Nyongesa HO. Context awareness in mobile computing: A review. Int J Machine Learn Appl. 2013;2(1), PAGES

[9] Almutairi, S., Aldabbas, H. and Abu-Samaha, A., 2012. Review on the security related issues in context aware system. International Journal of Wireless & Mobile Networks, 4(3), p.195.

[10] B. Ahmed, "Security and Privacy in context aware computing inside a hospital," JOURNAL NAME, 2015.

[11] Emmanouil Magkos, "Achieving privacy and access control in pervasive computing environments," JOURNAL NAME, 2011.

[12] P.Jagtap, "privacy preserving in context aware systems.," JOURNAL NAME, 2011.

[13] AUTHOR NAME, User Privacy Framework for Web-of-Objects based Smart Home Services International Journal of Smart Home Vol. 9, No. 5 (2015), pp. 61-72

[14] Syed M., Jalil A., Asif S. and Fayyaz K.,2015, Solving the Challenges of Pervasive Computing, University of Gujrat, Gujrat, Pakistan IS THIS ARTICLE OR MSC THESIS?

[15] E. Toch, "Crowd sourcing privacy preferences in context aware applications," JOURNAL NAME, 2012.

[16] S. Ackerman, "privacy in pervasive environments: next generation labeling protocol," JOURNAL NAME, vol. 8, no. 6, 2014.

[17] Wouter Bokhove, "Context-Aware adaptive privacy requirements," JOURNAL NAME, 2011.

[18] Mariappan, G. and Dhanabalachandran, M., 2014. Privacy Enhanced Pervasive Computing Model with Dynamic Trust and Security. Research Journal of Applied Sciences, Engineering and Technology, 7(23), pp.4872-4876.

[19] Boukerche, A. and Ren, Y., 2008. A trust-based security system for ubiquitous and pervasive computing environments. Computer communications, 31(18), pp.4343-4351.

[20] Latif, M.A., Ullah, F., Lee, H., Ryu, W. and Lee, S., 2015. User privacy framework for web-of-objects based smart home services. International Journal of Smart Home, 9(5), pp.61-72.

[21] Cornwell, J., Fette, I., Hsieh, G., Prabaker, M., Rao, J., Tang, K., Vaniea, K., Bauer, L., Cranor, L., Hong, J. and McLaren, B., 2007, March. User-controllable security and privacy for pervasive computing. In Eighth IEEE Workshop on Mobile Computing Systems and Applications (pp. 14-19). IEEE.

[22] Stephen, I.R., Charles, P.J. and Kumar, S.B.R., 2014. A review on privacy control techniques in context-aware web services. International Journal of Advanced Research in Computer Science & Technology (IJARCST'2014) 2: 3, 222, 225.

[23] Gaud, N., Deen, A. and Silakari, S., 2012, November. Architecture for discovery of context-aware web services based on privacy preferences. In 2012 Fourth International Conference on Computational Intelligence and Communication Networks (pp. 887-892). IEEE.

[24] Yau, P.W. and Tomlinson, A., 2011, October. Towards privacy in a context-aware social network based recommendation system. In 2011 IEEE Third International Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third International Conference on Social Computing (pp. 862-865). IEEE.

[25] Dehghantanha, A., Mahmod, R., Udzir, D.I. and Zukarnain, Z.A., 2009. UPEM: User-centered privacy evaluation model in pervasive computing systems. Ubiquitous Computing and Communication Journal, 4(4).

[26] Schaub, F., Könings, B., Dietzel, S., Weber, M. and Kargl, F., 2012, September. Privacy context model for dynamic privacy adaptation in ubiquitous computing. In Proceedings of the 2012 ACM Conference on Ubiquitous Computing (pp. 752-757).

[27] Chakraborty, S., Raghavan, K.R., Johnson, M.P. and Srivastava, M.B., 2013, February. A framework for context-aware privacy of sensor data on mobile systems. In Proceedings of the 14th Workshop on Mobile Computing Systems and Applications (pp. 1-6).

[28] Ackerman, M.S., 2014. Privacy in pervasive environments: next generation labeling protocols. Personal and Ubiquitous Computing, 8(6), pp.430-439.

[29] Pingley, A., Yu, W., Zhang, N., Fu, X. and Zhao, W., 2009, June. Cap: A context-aware privacy protection system for location-based services. In 2009 29th IEEE International Conference on Distributed Computing Systems (pp. 49-57). IEEE.

[30] Lederer, S., Dey, A.K. and Mankoff, J., 2012. A conceptual model and a metaphor of everyday privacy in ubiquitous computing environments. Computer Science Division, University of California.

[31] Amini, M. and Zokaei, S., 2013, October. A context-aware access control model for pervasive computing environments. In The 2017 International Conference on Intelligent Pervasive Computing (IPC 2017) (pp. 51-56). IEEE.

[32] Schaub, F., Könings, B., Dietzel, S., Weber, M. and Kargl, F., 2012, September. Privacy context model for dynamic privacy adaptation in ubiquitous computing. In Proceedings of the 2012 ACM Conference on Ubiquitous Computing (pp. 752-757)

[33] Boukerche, A. and Ren, Y., 2008. A trust-based security system for ubiquitous and pervasive computing environments. Computer communications, 31(18), pp.4343-4351.

[34] Sharma, S., 2017, February. A secure reputation-based architecture for MANET routing. In 2017 4th International Conference on Electronics and Communication Systems (ICECS) (pp. 106-110). IEEE.

[35] Kapitsaki, G.M., 2013, June. Reflecting user privacy preferences in context-aware web services. In 2013 IEEE 20th International Conference on Web Services (pp. 123-130). IEEE.

[36] Sievers, M., Madni, A.M., Pouya, P. and Minnichelli, R., 2019, October. Trust and Reputation in Multi-Agent Resilient Systems. In 2019 IEEE International Conference on Systems, Man and Cybernetics (SMC) (pp. 741-747). IEEE.

Appendix

```
package gmpmps;

import Archive.RequestReputation;
import Configuration.Aura;
import Entities.Node;
import Entities.PersonalAura;
import Entities.SocialAura;
import Entities.ThirdPartyAura;
import Evaluation.PreferenceSelection;
import Transaction.Request;
import java.util.ArrayList;
import java.util.Random;

public class GMPMPS {

   //create the auras
   Aura personal = new Personal Aura();
   Aura social = new SocialAura();
   Aura thirdParty = new ThirdPartyAura();

   //nodes list
   ArrayList<Node> nodes = new ArrayList<>();
   //reputations list
   ArrayList<RequestReputation> reputations = new ArrayList<>();
   //requests list
   ArrayList<Request> requests = new ArrayList<>();

   //preference selector reference
   PreferenceSelection selector = new PreferenceSelection();

   /**
    * @param args the command line arguments
    */
   public static void main(String[] args) {
      new GMPMPS();
   }
```

```
    public GMPMPS() {
        //create and configure auras
        this.configureAuras();
        //create and configure nodes
        this.configureNodes();
        System.out.println("LIST OF NODES");
        System.out.println("=============");
        for (int i = 0; i<nodes.size(); i++){
System.out.println(nodes.get(i).toString());
        }
        //create requests and store reputation (sample)
        this.sampleRequests();
        System.out.println("LIST OF REQUESTS");
        System.out.println("=============");
        for (int i = 0; i<requests.size(); i++){
System.out.println(requests.get(i).toString());
        }
        this.sampleReputations();
        System.out.println("LIST OF REPUTATIONS");
        System.out.println("=============");
        for (int i = 0; i<reputations.size(); i++){
System.out.println(reputations.get(i).toString());
        }
        //create and send request
        Random rand = new Random();
        Request testRequest = this.requests.get(rand.nextInt(this.requests.size()));
        double value = this.selector.calculateWeightedAverage(testRequest, this.reputations);
        System.out.print("CALCULATED VALUE  " + value);
              //check response[
        if(value==-1){
            System.out.println("No Reputation");
}else if(value >= this.personal.getAutoWeight()){
            System.out.println("Auto/ Go ahead");
}else if(value >= this.personal.getManualWeight() && value < this.personal.getAutoWeight()){
            System.out.println("Manual/ User intervention");
}else{
            System.out.println("Block/ Deny service");
        }
        //store reputation
    }
        public void sampleRequests(){
for(int i=0;i<500;i++){
            Request request = new Request(i, "REQ_"+i, 1);
            this.requests.add(request);
        }
    }
```

```
   public void sampleReputations(){
for(int i=0;i<5000;i++){
        Random rand = new Random();
        RequestReputation reputation = new
RequestReputation(this.nodes.get(rand.nextInt(this.nodes.size())),
              this.requests.get(rand.nextInt(this.requests.size())), Math.abs(rand.nextInt()%2));
this.reputations.add(reputation);
      }
   }

   public void configureAuras() {
this.personal.setAutoWeight(50);
this.personal.setManualWeight(20);
this.personal.setBlockWeight(0);

this.social.setAutoWeight(50);
this.social.setManualWeight(40);
this.social.setBlockWeight(39);

this.thirdParty.setAutoWeight(70);
this.thirdParty.setManualWeight(60);
this.thirdParty.setBlockWeight(59);
   }

   public void configureNodes() {
       for (int i = 0; i< 5; i++) {
        Node node = new Node(personal, (long)(Math.floor(Math.random()*100)), "SK", "Saba
Kebede");
this.nodes.add(node);
      }
       for (int i = 0; i< 150; i++) {
        Node node = new Node(social, (long)(Math.floor(Math.random()*100)), "ABC", "Contact" + (i +
1));
this.nodes.add(node);
      }


      for (int i = 0; i< 250; i++) {
        Node node = new Node(thirdParty, (long)(Math.floor(Math.random()*100)), "XYZ", "Org" + (i +
1));
this.nodes.add(node);
      }
   }

}
```