Mehran University Research Journal of Engineering & Technology
Vol. 37, No. 2, 241-256, April 2018
p-ISSN: 0254-7821, e-ISSN: 2413-7219
DOI: 10.22581/muet1982.1802.02

Dissecting the Security and Protection Issues in Pervasive Computing

QAISAR JAVAID*†, HUMERA YASMEEN**, MUNAM ALI SHAH**, MUHAMMAD KAMRAN***, AND ADNAN SOHAIL****

RECEIVED ON 18.07.2016 ACCEPTED ON 29.05.2017

ABSTRACT

Human beings reflect nomadic behaviour as they keep on travelling place to place whole day for personal or organizational purposes. The inception of modern networking technologies and the advent of wide range of applications in terms of services and resources have facilitated the users in many ways. The advancements in numerous areas such as embedded systems, WN (Wireless Networks), mobile and context-aware computing, anticipated pervasive computing dominated the human communication at large. Pervasive computing refers to the environment where information is accessible anywhere and anytime while existing system is invisible to the user. On the other hand, the invisibility of pervasive computing is also a problem in its adoption as users are unaware when and what devices collect their personal data and how it is being used. It has caused new security chaos as the more information about user is collected the more privacy and security concerns it raises, thus, the pervasive computing applications became key concern for user. This paper is aimed at analyzing the security and protection issues that arise while traveling from place to place connected with wireless mobile networks. The paper reviews many existing systems that offer possible security to pervasive users. An easy, precise and relative analysis and evaluation of surveyed pervasive systems are presented and some future directions are highlighted.

Key Words: Mobile Environment, Mobile Computing, Pervasive Computing, Ubicomp, Ubiquitous Computing, Pervasive Computing Environment.

1. INTRODUCTION

Technology has changed the formation of communication world. According to the needs of society and industry, the modern day has witnessed bursting advancements in the applications of communication technology. The functionalities of mobile devices are increasing day-by-day and today technology has shrunken the world as illustrated in **Fig. 1**. The advance computing capability of mobile devices made it possible to communicate where ever and whenever required. This computing capacity available in most of the daily use devices is characterized as pervasive computing. Pervasive computing is often referred as mobile computing or nomadic computing.

†Corresponding Author (E-Mail: qaisar@iiu.edu.pk)
* Department of Computer Science & Software Engineering, International Islamic University, Islamabad.
** Department of Computer Science, COMSATS Institute of Information Technology, Islamabad.
*** Department of Distance Continuing & Computer Education, University of Sindh, Jamshoro.
**** Department of Computer Science, Iqra University, Islamabad.

A term "Pervasive" comes near to the impression of ubiquity or submerging [1]. Hence, the "pervasive network" echoes ubiquitous network or nomadic network. Pervasive devices are intelligent objects that recognize other communicating devices automatically. The nomadic user has "anywhere and anytime" access to the world-wide grid irrespective of time and place. Over the past few years, nomadic computing has taken over the world. In today's hustle bustle of life, people move around with their mobile devices from place to place taking benefit of wide variety of services and resources. Pervasive computing includes freedom of location, motion, and platform and with extensive access to remote files, systems and services. These devices are replacing desktop computers with features like increased memory, processing power and with the support to vast variety of functions. To obtain these services, more private information is needed thus it is important to keep these devices secure. Regrettably, security of nomadic systems has not caught pace with nomadic trends. This vital asset of users is becoming more vulnerable to attacks therefore, valuable information on such networks and systems is at risk. Security is the main concern to protect the nomadic devices from the attacks [2].

When people get addicted to new technology, they expect its accessibility everywhere which results in reliance on the technology at large. Millions of mobile users travel from one place to another i.e. home, office, shopping mall, and hospital etc. they take their electronic companions with them everywhere. Thus, because of constant relocation from one station to another, vulnerabilities creeps up too with the reliability of the other environments available, as well as that of other devices connected within that environment, a user may accidentally bring in some threats such as viruses, worms etc [3]. Most of the existing security paradigms are mainly concentrating on better verification, routing, and stronger encryption. There exists a possibility that verified but virus affected devices could still have access to the network resources and infect other devices connected to the network.

FIG. 1. COMPUTING ENVIRONMENT TODAY

The main objective of this paper is to review the possible security and user's data privacy issues that arise in PCE (Pervasive Computing Environment), privacy management challenges, analyze existing pervasive computing architectures/models and evaluate the best among them on the basis of privacy management parameters. This paper is organized as follows. Section 2 provides a discussion on security and privacy threats in PCE. Section 3 presents challenges to privacy management techniques. In section 4 existing architectures of PCE are overviewed. Section 5 analyzes the architectures on the basis of privacy management parameters. In section 6, the work done so far is discussed and suggestions regarding some open issues are given before the paper is concluded in Section 8. At the end, some contributions are acknowledged.

2. SECURITY AND PRIVACY

Security is the main concern as the nomadic devices and nomads are increasing in number. Nomadic devices are introduced to new wireless environments in which they can suffer weak security. Following are some security threats that may occur in PCE and security needs to protect PCE.

2.1 Security Threats

Data Locality: When sensitive information is being passed over to the network, there is a great need to take high security measures. Even if the data is not that much sensitive but it is a users' significant asset. In case of data failure and absence of backup or recovery measures, organization may be at a great risk [4].

Wi-Fi Sniffing: A number of hardware and software devices are available to act as Wi-Fi sniffer. Through Wi-Fi sniffing, anyone can monitor either the location of device or the activity being done [4].

Wireless Communication: Communication over WN is more uncovered than communication over wires. In wireless communication, media is open and vulnerable to attacks. Data broadcasted through air is hard to control than the data that is accessible to only respective users [4].

Session Hijacking: Session hijacking is also known as cookie hijacking. It is the manipulation of a session key by gaining an unauthorized access to user information and services. This threat is of great concern in today's computing environments since the advancement of mobile banking is more prone to this type of threats [2].

Insecure Connectivity: Suppose a person goes to a shopping mall, restaurant etc. and because of mobile phones and forever connectivity has become a part and parcel of life, the devices of that person try to connect to the available network hence, ensuring secure connectivity is mandatory. Every person may not always be carrying a laptop with him but a mobile phone is must, which supports the fact that mobile devices are larger in number. Although, Wi-Fi is secured with passwords, still more susceptible to sniffing and other attacks, which is not as easy with cellular networks. Thus, they are more prone to security threats [4].

Web Browsing for Handheld Devices: Almost all mobile devices have the support for web browsing. This makes malware, spyware and other such threats easily infect the mobile devices as users unknowingly click on provided links while accessing websites on their phones [5].

Enhanced Socializing: Increase in social networking results in increased disclosure of private information to the "public" world. Suspicious links are available on social networking sites that can smoothen way for viruses to enter into a user's mobile device and hack their important details [4].

Location Services: Tracking location has become quite easy using GPS (Global Positioning System) available in all the smartphones. This has further made crime easy. Lack of privacy as well as security is the result of being tracked by location services all the time [6].

2.2 Security Needs

Security Policy: Policies define what information/data needs protection and how it will be provided. It must define how users are authenticated, type of information allowed to store, what to install, which resources used when connected with different privileged access, what kind of disciplinary actions be taken in case of violation of policy etc. [4].

Confidentiality: Users' data should be protected from loss of privacy. To ensure confidentiality few steps should be placed in consideration like encryption and VPN [2].

Integrity: Data should be protected against unauthorized modification. Electronic signatures can be used to secure messages over the network that guarantee the safety of content and also identity of the sender [4].

Firewall: One of the commonly used mechanisms for security is a firewall. Mechanism contains lists of permitted and non-permitted traffic.

Anti-Virus Software: Anti-virus is common and important mechanism to ensure security. It scans downloaded files, emails and removes malicious codes from files if found

File Protection on Device: Important files on devices should be encrypted and marked as "private" and hide them from unconcerned users, which makes files hidden for malicious users. These files should be password protected to avoid unauthorized access [5].

Secure Interoperability: As mobile networks are expanding and making interoperability and interaction between different organizations possible. These interactions need to be secure enough so that the sensitive data remain under cover [4].

Transparency: In nomadic environment, each entity must be authenticated transparently and acquire rights in transparent way [5].

Flexibility: New mechanisms for authorization and identification have been introduced over the past few years [5]. Mobile networks should be flexible to integrate these mechanisms.

Privacy Protection: In pervasive environment, user's sensitive information can be accessed and misused. To avoid such possibility, the user's devices must have the authority to recognize the environment in which they are located, and to evaluate its degree of confidence [2].

Security Levels: For each session over the network, the user should get access permission. High level security will be required for critical data accessing [4].

3. CHALLENGES TO PRIVACY MANAGEMENT MODELS

In this section, the research work is presented that concentrates on the number of challenges that occur in pervasive environment and their possible solutions to provide security to users.

Un-Noticeability: The ultimate objective of pervasive computing is to be un-noticeable. As in pervasive computing, devices are embedded and are 'intelligent' that can convey and collect user information. This intelligence feature lowers the observable quality of PCE. Absurdly, this same quality of PCE may also conquer the user privacy without his discern. This evacuates the user with a restricted control over sensitive information and to respect others' privacy as well. This disruption cannot be managed and forced through communal or administrational command. So, some measures should be taken to keep stability between user privacy and usability [7].

Location Reliance: Pervasive computing provides services to the users that require information about user's location. For example, while user travelling to a new place navigation maps are accessed to provide information about some services such as nearby restaurants. User has to make his location accessible to the service provider to gain advantage of these location centered services. Later, this obtained location data can be maltreated. There is also need for services to provide some flexible approaches to define different location privacy policies according to certain condition [8].

Context Reliance: Pervasive computing applications also rely on some contextual information. This context information may contain GPS coordinates, user preferences, user profiles, wireless device type, system time etc. The context-aware system uses a set of information which differs in privacy requirement level at times, making difficult to provide sufficient protection. There are no sufficient protocols to insure security for contextual information [9].

Contribution of Service Provider: Service provider has a critical and an important role being the maintainer and preserver of user data. There is the possibility of ill-use of user's sensitive data by the devices of service provider. Internationally some rules are specified that communicates objective, maintenance and receivers of data of each service provider request. But coming to reality it is difficult to ensure that these rules would not be violated [9].

Possession Deficiency: In traditional computing system, users have some specific access control and privileges to resources. In contrast, user enters and leaves PCE frequently and shares resources. Therefore, user has no privilege over the resources making it difficult to implement privacy controls [10].

Privileged Access Regulation: There must be some defined control of access rights to the confidential information in PCE. It is a challenging problem to control the access rights of users in diverse environment. At a time, user may be interacting with numerous smart devices and service providers. Since there is no guarantee of being un-maliciousness of these devices, hence, privacy of user maybe compromised [11].

Access Strategy Regulation: Some strategy must be defined to control access to user's confidential data. How user data is accessed and transmitted in diverse environment of PCE [11]**.** Although it is difficult to ensure fool proof security of user's sensitive data but some measures should be taken to define policies in regard to protect user's information.

Resources Taxonomy: In pervasive environment where users share resources, surplus parties could access the confidential information triggering leakage of user information and violating the user privacy. There must be some parameters taken to promise the users that resource sharing will avert private information outflow [9].

Data Maintenance Authority: In PCE, user data can be spontaneously composed together and kept over extended time span. User private information is quite respected that must be protected against any ill-use and revelation. To achieve this purpose, data may be distributed at different systems thus data persistence is as important as data revelation [10]. PCE must define some tools to control data revelation and ensure data persistence for example, may be by placing some time constraints.

Constraints Definition: In a PCE, there must be some defined constraints on access rights. Sometimes to gain access to a specific service a user may have to tradeoff the level of privacy. Possessors of information should be given suitable criteria to specify the circumstances under which their data can be retrieved.

In a PCE, to gain access to a certain service there must be some criteria defined for granting access permission. A number of policies could be defined and the conditions and rules to get permission to gain access to particular service(s) [3].

Service Access Approval: In the era of detection technologies context data may be provided which contains location information, user profiles, time etc. user may want to maintain the confidentiality of his data and want to know who can access what and how it is being used [10].

Information Usage Monitoring: The communication takes place in PCE is visible to service provider. To guarantee non-leakage of user data, SP must require only essential data for a specific task and user should offer just required data [10]. The decision must be taken earlier about the data sharing among users and service providers.

Data Concealment Assurance: The assemblage and storage of information sets a trial to privacy of user. Information should be secured from third party access and any misuse by the ISP, be restricted and such information should be hold for future referencing [10]. When data is transmitted, it should be transmitted to the supposed recipient. No control over data transmission means no control over privacy.

4. EXISTING SYSTEMS OF PERVASIVE COMPUTING

This section reviews some of the work that has been done so far for ensuring the security and privacy of pervasive devices as the new technology makes its way. Primary requirement in pervasive computing is to provide sufficient security and ensured privacy everywhere and anytime to all nomadic users. By ensuring the privacy of nomadic systems, security could inevitably be achieved. Over the years, a number of schemes, methods and models have spoken about some prominent problems of security and privacy in pervasive environments. Taxonomy of these systems is presented in Fig. 2 and summary of respective systems is presented in detail in Table 1.

Privacy Sensitive Information dilUting Mechanism: Cheng et. al. [12] states two techniques in their paper "Protection of Privacy in Pervasive Computing Environment". The first method they presented is a technique called PSIUM (Privacy Sensitive Information dilUting Mechanism) which is capable to avert the misuse of user information by an ISP (Internet Service Provider). It uses a true or false sensor data for protection from ISP. In second method, subtle information is being protected by keeping the continuously varying traffic values so that information is not revealed to the attacker by analyzing the traffic. A device, which uses PSIUM, sends several locations based request messages to ISP and among those only one contains true location of user. The device knows about the true information and makes it available to the user. PSIUM holds false data as well so that it may help identify the actual message otherwise it will be difficult to

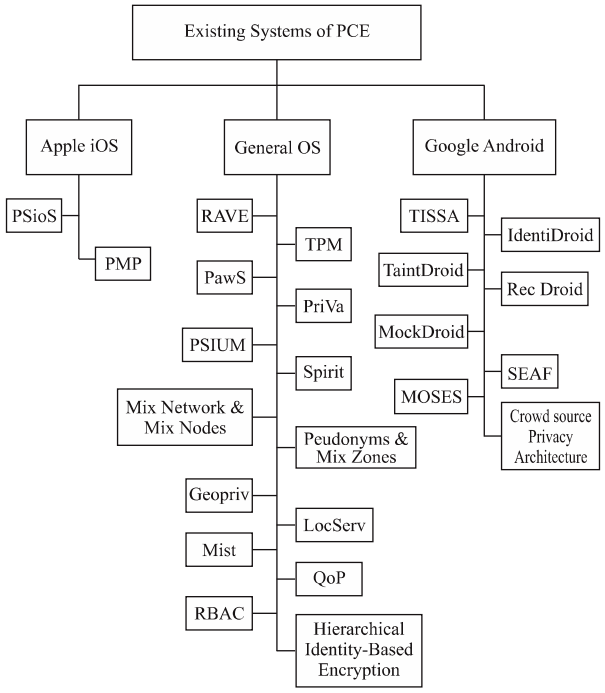

FIG. 2. TAXONOMY OF EXISTING PCE SYSTEMS

distinguish between true and false information for the ISP. This false data is produced by using the previous locations that user has had used. The strong side of PSIUM is that it protects the ill use of users' data by ISP and preserves the quality of the service as well. Its weak side is that increase in number of queries results in increase in cost of attaining results and communication between user and ISP is susceptible to attack [12].

Spirit: Spirit is a modern location based system with middleware event driven applications which generate events when an entity enters or exits some predefined space. Some specific locations are defined in applications and whenever an entity enters that particular defined space, application receives callback of occurring of an event from middleware. Communication between user and application is indirect in nature [13]. Currently, the

TABLE 1. SUMMARY OF EXISTING SYSTEMS

	Mechanisms	Motivation/ Approach	Advantages	Limitations
General OS	RAVE	■ Designed to support people who are at geographically distinct location.	■ Users can control who can establish a link to them and what sort of linking is permissible. ■ 'Feedback' alerts users of data type being send and who has access to that data. ■ Provides a privacy control at all levels of distinction.	■ Awareness, privacy, and interference margins can easily be violated.
	TPM	■ Implements access rights without sharing user's identities to third parties. ■ Authenticate a user by sending a challenge to the device, which is then signed by the access requester.	■ Provides vigorous security against third party intrusion. ■ Ensure privacy using operation signing.	■ Ties a user to a single computer. This makes multiple device use impractical, ■ Key management is complex.
	PawS	■ Provides tools to the users to let them protect their sensitive information help others respect them. ■ It is based on respect, legal and social norms.	■ User has a control over the privacy policies. ■ User has the authority to either allow or reject an access request. ■ Confidential data is secured.	■ No technical approach is applied. ■ Needs user intervention at each service request.
	PriVA	■ Avoid information leaks while sharing resources and information among the users. ■ It has a default policy for particular resources. ■ Default policies are un-changeable.	■ If sharing a resource is undesirable, user can tag it as 'non-sharable'. ■ Policy flexibility achieved because of addition of Customized policies.	■ Lack clear vision to cope with the very open and dynamic nature of the environment.
	PSIUM	■ To avert the misuse of user data by an Internet Service Provider (ISP). ■ Subtle information is being protected by keeping the continuously varying traffic values so that information is not revealed to the attacker by analyzing the traffic.	■ It protects the ill use of users' data by ISP ■ Preserves the quality of the service as well.	■ Increase in cost of attaining results due to large number of queries ■ Communication between user and ISP is susceptible to attack
	Spirit	■ System with middleware event driven applications which generate events when an entity enters or exits some predefined space.	■ Support mobile users in mobile environments by making all kinds of information about the environment accessible over the network. ■ Possible for users to control access to their own information.	■ Limited number of software resources is incorporated. ■ Communication between user and application is indirectly.
	Mix Networks and Mix Nodes	■ by offering a store-and-forward network support anonymous communication. ■ A mix node accepts input of n-equal length packets and reorders them by applying some metric before forwarding them to destination.	■ Provides protection ■ This system delivers best measures when sending are in large number. ■ Provide privacy protection even in indiscreet environment.	■ Communication between user and ISP is still vulnerable to attack.
	Pseudonyms and Mixed Zones	■ It is same as the 'Mix Networks and Mix Nodes' technique. ■ Entities participating in communication are given 'nicknames' to identify them.	■ The ability to ensure privacy while user and ISP communication takes place.	■ Pseudonyms can be tracked. ■ Tougher to device them in practice because of its complexity.
	Geopriv	■ To securely gather and transfer user location info and ensures to protect privacy of entities. ■ Location objects are created which encapsulates user location information and privacy preferences alongside it.	■ Location objects are digitally signed to protect data from any sort of distraction. ■ Offers greater accountability.	■ No practical implementation yet.

middleware offers direct access to all location based events but, it can be possible for users to control access to their own information. The strong side of this model is that it supports mobile users in mobile environments by making all kind of information about the environment accessible over the network and make it possible for users to control access to their own information. The weak side is that the limited number of software resources can be incorporated and the communication between user and application is indirectly carried out.

Networks and Mix Nodes: A mix network offers anonymous communication by offering a store-and-forward network. The network carries some nodes for message routing along with some special nodes called 'mix nodes' [14]. In this network, a mix node accepts input of n-equal length packets and reorders them by applying some metric before forwarding them to destination. This method provides elimination of existence of any link between incoming and outgoing message and hence provides protection ultimately. This system delivers best measures when sending nodes are in large number. As larger the anonymity set results in greater anonymity offered hence provide privacy protection even in indiscrete environment. But communication between user and ISP is still vulnerable to attack [14].

Pseudonyms and Mixed Zones: This technique is same as the 'Mix Networks and Mix Nodes' technique, the only difference is the entities participating in communication are given 'nicknames' to identify them. The advantage of this model is the ability to ensure privacy while user and ISP communication takes place. Pseudonyms can be tracked and tougher to device for translating them in practice because of its complexity [15].

Geopriv: The motivation behind Geopriv is to securely gather and transfer user location information while ensuring the protection of privacy of the entities involved. Myles et. al. [16] in their paper describe Geopriv scheme in which location based objects are created which encapsulates user location information and privacy preferences alongside it. These objects are digitally signed to protect data from any sort of distraction. This scheme could offer greater accountability but practically this scheme has not been implemented yet, Compbell et. al. [17].

LocServ: LocServ serves as a middleware service between applications and location tracking machineries. Myles et. al. [16] in their paper "Preserving Privacy in environments with location-based applications" describes LocServ applications use a number of systems where users can identify location query by using any of the location model (symbolic or geometric) then service resolve query using any of technology that LocServ understands. Applications works independent of the technologies used. This type of service allows users to have control over the amount of location information that can be released but it depends upon user for location query.

Mist: Roy et. al. [16] proposed a model that guarantees protection of both location information and user's privacy. Anonymous communication for location-based applications and user is provided by Mist. In this method, location information is preserved from the identity of the entity. Mist builds an encryption protocol for communication, thus allows users to maintain their privacy while gaining access to the service. A protocol is built on routers which are organized on hierarchical levels. The level of privacy is customizable. User can specify a protection level for information flow over the network by simply making a choice to which router to connect to. Router at highest level of hierarchy provides a highest privacy protection. Advantage of this model is that it guarantees protection of both location information and user's privacy and the level of privacy is customizable. Disadvantage is that if the user chooses a connecting router at a lower hierarchy then the protection is lower too.

Privacy Awareness System: PAWS (Privacy Awareness System) protect privacy of user and requires others to respect that privacy as well. PAWS impose restrictions upon users' information usage by ISP. It includes information collecting tools and processing techniques that require ISP to negotiate the policies involved in information collection. ISP must keep the user aware of such policies so that user can control propagation of private information on his own[18]. PAWS cannot enforce information constraints between ISP and user, but only communicate hence, it relies on trust model. PAWS cannot provide protection wholly where trust is not certain. No technical protection model is proposed rather based on moral, social and authorized standards [19].

Quality of Privacy: As the name suggests QoP (Quality of Privacy)architectures provide a mechanism that balances the privacy measures between the user and ISP. Quantitative parameters are used to manage the level of privacy provided to user. These quantitative parameters are based on five contextual variables: location, identity, access, activity and persistence [20]. The parameters can determine the cost to avail the services provided by ISP. In QoP, the information shared by the user with the pervasive environment is controlled according to the level of negotiation between the user and the service provider. But the perception of anonymity is dependent upon quantitative parameters.

RAVE: RAVE is a new system designed to facilitate individuals geographically dispersed, but work on some common interests together. They can use several ways for distributing or receiving their audio-video content to/ from others. The users can control who can establish a link to them and what sort of linking is permissible. Feedback, as the name suggests, provided by this system to the users informing about the type of data is being sent and who can access such data. Moreover, one benefit of RAVE is to provide a privacy control to user at all levels by quickly making decisions about permission granting to the users for defined service. Its downside is that the awareness, privacy, and interference margins are violated easily [21].

The Trusted Platform Module: The TPM (Trusted Platform Module) is a trusted hardware way-out for pervasive computing. TPM device access rights where user identity is not revealed to other group of people. A mobile user authentication process is preceded by sending a challenge to the device and then signing by the access requestor hence making it digitally secure. This technique offers high security for user private information where there is a possibility of third-party stealing information. The outward entity will be unable to authenticate the signed mark and therefore not able to enter a secure pervasive computing environment [22]. The good point of this approach is that it provides vigorous security against third party intrusion and ensures privacy using operation signing but this makes its use on multiple device impractical and key management is complex.

Layered Model: Blain et. al. [23] proposed a layered model in his paper "Keeping Ubiquitous Computing to Yourself: a practical model for user control of privacy". This model has identified four layers, through which a user must navigate, that are regulatory regimes layer, ubiquitous computing services layer, data layer, and user layer [22]. Regulatory regimes layer defines regimes they are currently in, ubicomp services layer specifies services that are required, data layer constitutes the data type being revealed, and user layer specifies user's privacy strategy. This model balances the user's privacy preferences and the privacy regulations that are applicable. It includes five types of user controlled 'noise' to protect location privacy. The rising issue of matching data and user layer guidelines for different monitoring systems was emphasized.

User-Centered Privacy Evaluation Model: Dehghantanha et. al. [24] proposed an evaluation method that assesses privacy models that were proposed earlier. This method assesses privacy models using three evaluation factors that are based on user control over private information, in how much detail privacy policies expressed, and unobtrusiveness of privacy mechanisms. It compares all the privacy models and represents privacy level of those models in matrix.

Pervasive Formal Privacy Language: Dehghantanha et. al. [25] introduced a PERFORM (Pervasive Formal Privacy Language) to draw user level privacy policies into real data level policies. The PERFORM defines events related to pervasive environments and features of pervasive environments**.** It is a formal language defining three terms i.e. requests, responses, and constraints. A request is a line of code that evaluates some conditions then, in result, performs some responses that may alter the related condition. A constraint is a set of specific situations upon which a decision is derived that directs where and when some specific activities should be allowed or banned.

Privacy Violation Avoider: PriVA **(**Privacy Violation Avoider) is a model targeting to ensure information non-leakage when communicating with other users or using shared resources. By default, there are some policies characterized by model which cannot be changed. If a user doesn't want to share a certain resource(s) he can do so by tagging that resource 'un-sharable' without going to indulge in making complex strategies. User can add further policies to default policies by selecting policies from list of policies defined. This model provides flexibility to users to define their own privacy policies and shared resources [26].

Hierarchical Identity-Based Encryption: HIBE **(**Hierarchical Identity-Based Encryption) offers a way to transfer context information with defined granularity level of information, abstracting the detail of information. Based on this granularity level, an access to certain information may be denied or evaluated before granting access. User who owns the information can set the granularity and associated privacy levels. This approach gives an open hand to users to define parameters in order to protect their data [27].

Role Based Access Control: Most extensively used method to govern authorized access to resources and services is RBAC (Role Based Access Control). Users are assigned roles and have certain privileges. To gain access to service or resource, they may have to compromise a bit of privacy. Restraints on privileges sometimes are responsible for the tradeoff between privacy level a user is granting and the service provided in result. Owners can state the circumstances to access their information. As there are large number of service providers and the users, thus, it is difficult to ensure protection to each. Therefore, it is impractical to implement it [27].

An abundant work has been done to make nomadic devices more secure, reliable, invulnerable, and immune to spiteful abuse [9]. As PDAs (Personal Digital Assistant) are ruling the world nowadays, most of the mobile devices' operating system is Android or iOS.

Taming Information Stealing Smartphone Applications: Zhou et. al. [28] introduced TISSA (Taming Information Stealing Smartphone Applications) which provides a privacy mode that permits the user to control a criterion upon which application can access the personal information. At runtime, granted access can be modified according to the scenario. It required few lines of code and had a negligible performance overhead. This application requires modification to the Android OS.

IdentiDroid: IdentiDroid is a customized Android OS proposed by Shebaro et. al. [29] which guarantees security that applications cannot ascertain a user. IdentiDroid takes two approaches. First approach is to shadows user and application data, information about device, and the resources used so that user identity could not be revealed. Second approach is to modify runtime

permissions of Android applications by change of modality. Their experiments showed that IdentiDroid guarantees better user anonymity than other previously proposed approaches and have negligible effect on applications of the device.

Android Runtime Security Policy Enforcement Framework: Banuri et. al. [30] proposed a framework that observes an application's behavior during its runtime. The framework is named as 'The Android Runtime SEAF (Security Policy Enforcement Framework) which notices application's permission patterns and aids in application validation. User is conversant of the hazardous behavior of application grounded on permission patterns' permutation. Initial examinations showed its insignificant performance overhead and found it reliable enough to be used in consumer market but it requires alteration to underlying Android OS.

TaintDroid: TaintDroid is an information flow tracking system for runtime privacy monitoring of smartphones proposed by Enck et. al. [31]. TaintDroid tracks the flow of user private data through third-party applications running on smartphones. It considers third-party applications as non-trust-worthy and monitors their behavior during execution how they use users' sensitive data. Enough of contextual information needed to analyze data to where it is sent and how personal is it. TaintDroid labels the privacy sensitive data source as taint and monitors its flow over the network. When data leaves the system, it notices taint label of data, its destination, and the application responsible for transmitting that data. This feedback notifies users and services about the suspicious applications. Performance overhead must be low and it was acknowledged that context based personal data could be tough to sense.

PSiOS: PSiOS concentrates to ensure security and privacy in iOS. It is a tool which provides a sandboxing (user or administrator defined) for each application running on iOS. Some popular iOS applications (e.g. Facebook, WhatsApp) are evaluated to validate the throughput and usefulness of PSiOS. It needs a modification to the native source code [32].

RecDroid: Rashidi et. al. [33] proposed RecDroid which is a framework for users to govern approval to the applications before they run for the very first time then receives commendations from expert users of the same application. User can take advantage of it to make correct decision regarding permission granting. Previously granted permissions can be modified later hence saving users from mischievous applications. Evaluation done on Android smartphone, framework proved to be viable and convenient to use.

Crowd source Privacy Architecture: Papamartzivanos et. al. [34] focus their work to evaluate applications that may threaten security and privacy of end user. As most of the applications now trending; not only put security at risk but also exposes personal information that is not essentially required for their operation. The authors propose a solution that can detects privacy information leakage through smartphone applications. End users and the concern authorities are informed of information leakage.

MockDroid: Beresford et. al. [35] proposed MockDroid which is a reformed model of Android OS in which user is asked about the access to a particular resource is given or not. The resource can be told as empty or unavailable. It lets the user to trade-off between performance and revelation of sensitive data to use application. If user denies the access to resource, application could still run but performance may suffer. This approach was successfully experimented on 23 applications running on Android OS. It requires amendment in Android source code.

MOSES: Security tools for smartphones provide partial shield wicked applications which results in serious threat to subtle corporate data stored in smartphone. A policy-based framework is proposed named MOSES imposing segregation of applications and data. Within the same

OS different virtual environments can define a separate security profiles for applications. Each profile is associated with some defined policies that who can access data and applications. Dynamically switching among the security policies is the fundamental distinction of MOSES. This framework disclosed trivial overhead in both battery and latency[12].

ProtectMyPrivacy: Agarwal et. al. [36] presented a design and execution of PMP (ProtectMyPrivacy) system proposed for iOS to identify access to user personal data. If user desires, it replaces user's data with anonymous data. PMP is a crowd source engine which facilitates the users to make privacy recommendations about certain application to ensure protection. They presented widespread access to the device identifier, address book, location, and music library in iOS. Some protection settings were recommended. It requires a modification to native code.

5. HYPOTHESIS ANALYSIS

Chin et. al. [37] conducted a user study consisting of 60smartphone users. They worked on the hypothesis that users avoid to use smartphones due to security and privacy apprehensions. They interviewed users on their willingness to perform certain tasks for verifying the hypothesis. Secondly analyzed how and why users select applications and what are their preferences. They suggested some opportunities to use those applications securely.

6. PERMISSION PATTERN PERMISSION

Liu et. al. [38] analyzed how users' data are grouped to define like-minded users and predict their permission patterns for future. Some permission patterns are too complex to conclude any analysis about them. They proposed that user must be asked to provide permission by choosing amongst different setting options. At run-time, these permissions can be modified. Users have a choice to "grant", "deny" or "request to be run-time driven" when permitting to recently downloaded application.

7. PERFORMANCE EVALUATION AND COMPARISON

This research covers many models/architectures (of general OS, Android, iOS) proposed earlier to provide security and ensure protection to user data and privacy in pervasive computing environments. Each has some advantages over the rest and some lacks some of the features that others offer. We summarized the methodology, advantages, and limitations of the respective architectures in Table 1. Furthermore, to evaluate the techniques used in previous architectures/ models are compared on the basis of number of challenges addressed in section III. The certain area considered in respective architecture is assigned 1 and 0 if is not available as shown in Table 2.

After that, the results are summarized simply by adding the number of 1's against each architecture. We get the concluding results in Table 3. This analysis is represented in Fig. 3. As a graph to make the comparison more visible. By looking at the graph, it can be concluded that PawS model has focused the most number of areas to provide secure and protected environment to pervasive users. Mist, QoP, RAVE have the same number of areas focused but is different from methodological point. PSIUM, Pseudonyms and Mixed-Zones, LocServ and Spirit have considered average areas to work for pervasive environment. Whereas,mixed network and mixed-nodes and Geopriv have fixed limited areas only.

8. OPEN ISSUES AND DISCUSSION

In this research paper, number of security threats and users' privacy needs in pervasive computing are discussed. This paper provides a summary of twenty-four different architectures proposed earlier which constitutes methodology/approach, advantages, and

limitations. This research work lists the thirteen parameters which need to be focused to ensure security and privacy of the nomadic user. Afterwards, different previously proposed architectures or models based on these parameters are analyzed and evaluated through graphical representation that the PawS has focused on maximum parameters.

Although, a lot of work has been done in this area but there is still a need to make PCE more secure for its users. As PawS is evaluated as the best approach among others but even PawS needs further improvement. Context and location reliance, constraint definition and service access granting should be considered to make PawS more consistent. It is analyzed that rules have been defined for ISP contribution in most of the proposed models but no rules or tools are proposed for resource sharing and data revelation. User contextual information is commonly collected but ambiguity of data usage policies are still a question mark. Based on this analysis, we suggest some criteria to gain more security, i.e. applications should ask permission for location and contextual data every time environment is changed, explicitly inform users about which data is accessed and how it will be used, policies defined on the misuse of user's data by ISP, third-party or any other concerned individual or group, make user an authority. It is always a trade-off as the fool-proof security cannot be achieved in diverse environment like PCE but it can be improved.

TABLE 3. SUMMARY OF AREAS OF CONCENTRATION

Architectures	Total Areas Considered
PSIUM	5
Mix networks And Mix Nodes	2
Pseudonyms and Mix-Zones	5
LocServ	6
Mist	7
Geopriv	4
Spirit	5
PawS	9
Quality of Privacy	7
RAVE	7

TABLE 2. SUMMARY OF EXISTING SYSTEMS

	Mechanisms	Motivation/ Approach	Advantages	Limitations
Google Android	MockDroid	■Reformed model of Android OS ■User is asked about the access to a resource ■Resource can be told as empty or unavailable	■ It is applicable ■ User has the granting authority	■ It requires amendment in Android source code ■ Performance may suffer ■ Tradeoff between performance and revelation of sensitive data.
	MOSES	■A policy-based framework ■Impose segregation of applications and data ■Different virtual environments can define a separate security profiles for applications ■Each profile is associated with defined policies	■ Dynamically switching among the security policies ■ Control who can access data and applications ■ trivial overhead in both battery and latency.	■ Specifying security policies could be an intimidating task for most of the non-IT minded users
	Crowd source Privacy Architecture	■Evaluate applications that may threaten security and privacy of end user ■Detects privacy information leakage through smartphone applications	■ A real-time privacy-flow tracking service ■ End users and the concern authorities are informed of information leakage ■ Stop the propagation of malware ■ Practical to implement.	■ Information tracked may be ill-used ■ Puts user privacy at risk by tracking process of user's information flow
Apple iOS	PMP	■A crowdsource engine for iOS ■To identify access to user's data ■Facilitates users to make privacy recommendations about certain application to ensure protection.	■ Allows users to contribute their privacy decisions	■ Requires a modification to native code
	PSiOS	■Ensure security and privacy in iOS. ■Tool that provides a sandboxing (user or administrator defined)	■ Significant throughput ■ Useful to evaluate applications	■ Needs a modification to the native source code

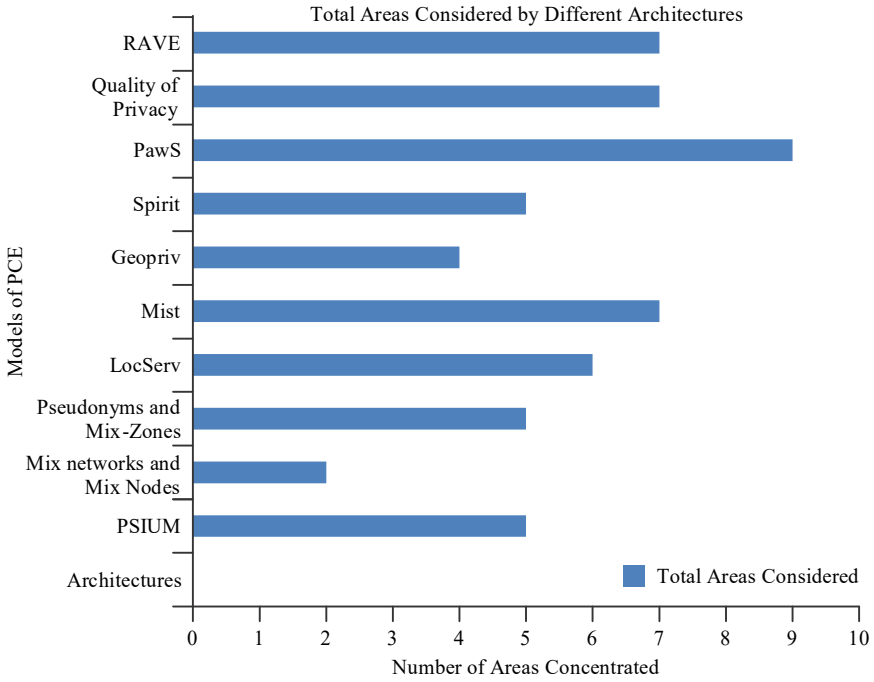

FIG. 3. GRAPH OF AREAS CONCENTRATED BY PCE MODELS

9. CONCLUSION

Where people adore benefits a pervasive computing accompanies, security and privacy of pervasive environment is a fundamental requirement. In this paper, numerous challenges for protecting user's sensitive data have been addressed. There had not been given much attention on the security and privacy protection of users' information in PCE since its emergence but this research paper focused on the key areas that need to be concentrated. Various existing systems are summarized and evaluated according to the number of key areas focused by these existing systems. Security and Privacy are the basic concern in PCE and it should be concentrated properly while designing pervasive computing applications so that better quality of service is provided to pervasive users.Hence, this paper summarizes the existing development in PCE environment and provides their qualitative comparison for advantages and limitations.

ACKNOWLEDGEMENT

Authors would like to acknowledge with thanks the anonymous referees for their useful suggestions that led us to enhance the quality of the paper. Authors are also thankful to the International Islamic University, Islamabad, and COMSATS Institute of Information Technology, Islamabad, Pakistan, for providing platform to carry out this research.

REFERENCES

[1] Beal, V., "Pervasive Computing", [Online]. Available:http://www.webopedia.com/TERM/P/pervasive_computing.html. [Accessed: 10th November, 2015].

[2] Vikas, S.S., Pawan, K., Gurudatt, A.K., and Shyam, G., Mobile Cloud Computing: Security Threats. Proceedings of IEEE International Conference on Electronics & Communication Systems, pp. 1-4, 2014.

[3] Langheinrich, M., "A Privacy Awareness System for Ubiquitous Computing Environments", Proceedings of 4th International Conference on Ubiquitous Computing, pp. 237-245, 2002.

[4] Kaur, N., "Delving into the Security Issues of Mobile Cloud Computing", International Journal of Computer and Communication System Engineering, Volume 2, No. 3, pp. 451-454, 2015.

[5] Djedid, M.N., "A Trust-Based Security Mechanism for Nomadic Users in Pervasive Systems", CoRR-Computing Research Repository - arXiv.org, pp. 2-3, 2012.

[6] Chou, T., "Security Threats on Cloud Computing", International Journal of Computer Science & Information Technology, Volume 5, No. 3, pp. 79-88, 2013.

[7] Pareschi, L., Riboni, D., and Bettini, C., "Protecting Users' Anonymity in Pervasive Computing Environments", 6th Annuual IEEE International Conference on Pervasive Computer Communication, pp. 11-19, 2008.

[8] Saha, D., and Mukherjee, A., "Pervasive Computing: A Paradigm for the 21st Century", Computer, Volume 36, No. 3, pp. 25-31 2003.

[9] Tentori, M., Favela, J., Gonzalez, V., and Rodriguez, M.D., "Supporting Quality of Privacy (QoP) in Pervasive Computing", 6th Mexican International Conference on Computer Science, pp. 58-65, 2005.

[10] Bhaskar, P., and Ahamed, S.I., "Privacy in Pervasive Computing and Open Issues", Proceedings of 2nd IEEE International Conference on Availability, Reliability and Security, Computer Society., pp. 147-154,2007.

[11] Hengartner, S.P.U., "Access Control to information in Pervasive Computing Environments", 9th Workshop on Hot Topics in Operating Systems, pp. 157-160, 2003.

[12] Cheng, T.J.G., and Zhang D., "Protection of Privacy in Pervasive Computing Environments", International Conference on Informatoin Technology, Coding and Computing, pp. 242-247, 2005.

[13] Beresford, S.F., "Location Privacy in Pervasive Computing", IEEE Pervasive Computer, Volume 2, No. 1, pp. 46-55, 2003.

[14] Beresford, S.F., "Location Privacy in Pervasive Computing", IEEE Pervasive Computet, Volume 2, No. 2, pp. 40-46, 2003.

[15] Obaidat, W.I., and Denko, M., "Pervasive Computing and Networking", John Wiley & Sons, 2011.

[16] Myles, D.N., and Firday, A., "Preserving Privacy in Envronments with Location-Based Applications", IEEE Pervasive Computer, Volume 2, No. 1, pp. 56-64, 2003.

[17] Campbell, R., Al-muhtadi, J., Naldurg, P., Sampemane, G., and Mickunas, M.D., "Towards Security and Privacy for Pervasive Computing", Proceedings of Software Security—Theories and Systems, pp. 1-15, 2003.

[18] Langheinrich, M., "A Privacy Awareness System for Ubiquitos Computing Environments", Proceedings of 4th International Conference on Ubiquitous Computing, pp. 72-74, 2002.

[19] Langheinrich, M., "A Privacy Awareness System for Ubiquitous Computing Environments", Proceedings of 4th International Conference on Ubiquitous Computing, pp. 237-245, 2002.

[20] Tentori, G.V.M.,Favela, M., and Rodriguez, M.D., "Supporting Quality of Privacy (QoP) in Pervasive Computing", 6th Mexican International Conference on Computer Science, pp. 58-67, 2005.

[21] Bhaskar, P., and Ahamed, S.I., "Privacy in Pervasive Computing and Open Issues", Proceedings of 2nd International Conferenceon Availability, Reliability Security, pp. 147-154, 2007.

[22] Kurkovsky, S., Rivera, O., and Bhalodi, J., "Classification of Privacy Management Techniques in Pervasive Computing", Pervasive Computer International Journal of Science Technology, Volume 11, No. 1, pp. 55–58, 2007.

[23] Blaine, A.P., Adam, K., and Nuseibeh, B., "Keeping Ubiquitous Computing to Yourself: A Practical Model for User Control of Privacy", International Journal of Human-Computer Studies, Volume 63, No. 1-2, pp. 228-253, 2005.

[24] Dehghantanha, Z.Z., Mahmod, R., and Udzir, N., "UPEM: User-Centered Privacy Evaluation Model in Pervasive Computing Systems", Ubiquitous Computert Communication Journal, Volume 4, No. 4, pp. 50-57, 2009.

[25] Dehghantanha, M.R., and Udzir N., "Towards a Pervasive Formal Privacy Language", IEEE 24th International Conference on Advvanced Information Network Applications, pp. 1085-1091, 2010.

[26] Asif, K.M., Ahamed, S.I., and Talukder, N., "Avoiding Privacy Violation for Resource Sharing in Ad hoc Networks of Pervasive Computing Environment", 31st Annuual International Conference on Computter Softwtware Application, Volume 2, pp. 269-274, 2007.

[27] Zhiguo, W., Jun'E, L., and Robert, H.D., "HASBE: AHierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing", IEEE Transactions on Information Forensics and Security, Volume 7, No. 2, pp. 743-754,2012.

[28] Zhou, Y., Zhang, X,. Jiang, X., and Freeh, V.W., "Taming Information-Stealing Smartphone Applications (on Android)", Proceedings of 4th International Conference on Trust and Trustworthy Computing, pp. 93-107, 2011.

[29] Shebaro, B., Midi, D., Bertino, E., and Oluwatimi, O., "IdentiDroid: Android Can Finally Wear its Anonymous Suit IdentiDroid/ : Android Can Finally Wear its Anonymous Suit", Transactions on Data Privavy, Volume 7, pp. 27-50, 2014.

[30] Banuri, H., Alam, M., Khan, S., and Manzoor, J., "An Android Runtime Security Policy Enforcement Framework", Ubiquitous Computer, Volume 16, No. 6, pp. 631-641, 2012.

[31] Enck, W., Cox, L.P., Gilbert, P., and Mcdaniel, P., "TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones", Proceedings of 9th USENIX Conference on Operating Systems Design and Implementation, pp. 1-6, 2010.

[32] Werthmann, T., Davi, L., Sadeghi, A., and Holz, T., "PSiOS: Bring Your Own Privacy & Security to iOS Devices Categories and Subject Descriptors", 8th ACM SIGSAC Symposium on Information, Computer and Communications Securirty, pp. 13–24, 2013.

[33] Rashidi, B., Fung, C., and Vu, T., "RecDroid: A Resource Access Permission Control Portal and Recommendation Service for Smartphone Users", ACM MobiCom Workshop on Securrity Privary Mobile Environment, pp. 13-18, 2014.

[34] Papamartzivanos, D., Damopoulos, D., and Kambourakis, D., "A Cloud-Based Architecture to Crowdsource Mobile Application Privacy Leaks", Proceedings of 18th Panhellenic Conference on Informatics, pp. 1-6, 2014.

[35] Beresford, A.R., Rice, A., and Skehin, N., "MockDroid: Trading Privacy for Application Functionality on Smartphones Categories and Subject Descriptors", 12th Workshop on Mobile Computing Systems and Applications, pp. 49–54, 2011.

[36] Agarwal, Y., and Hall, M., "ProtectMyPrivacy: Detecting and Mitigating Privacy Leaks on iOS Devices Using Crowdsourcing Categories and Subject Descriptors", 11th Annual International Conference on Mobile Systems, Applications, and Services, Volume 6, pp. 97-110, September, 2014.

[37] Chin, E., Felt, A.P., Sekar, V., and Wagner, D., "Measuring User Confidence in Smartphone Security and Privacy", 8th Symposium on Usable Privacy and Security, No. 1, pp. 1-16, 2012.

[38] Liu, B., and Sadeh, N., "Reconciling Mobile Application Privacy and Usability on Smartphones: Could User Privacy Profiles Help?," 23rd International Conference on World Wide Web, pp. 201-212, 2014.