Egyptian Informatics Journal (2015) **16**, 151–166

Cairo University

Egyptian Informatics Journal

www.elsevier.com/locate/eij
www.sciencedirect.com

ORIGINAL ARTICLE

A multi-agent approach: To preserve user information privacy for a pervasive and ubiquitous environment

Chandramohan Dhasarathan *, Sathian Dananjayan, Rajaguru Dayalan, Vengattaraman Thirumal, Dhavachelvan Ponnurangam

Department of Computer Science, Pondicherry University, Pondicherry, India

Received 8 December 2013; revised 19 January 2015; accepted 16 February 2015
Available online 23 March 2015

KEYWORDS

Pervasive computing;
Privacy;
Security;
Multi-agent;
Hash Diff Anomaly Detection and Prevention (HDAD)

Abstract Cloud user's data are getting insecure in current technological advancement. This research focuses on proposing a secure model to maintain the secrecy in a cloud environment using intelligent agent. This paper presents an intelligent model to protect user's valuable personal data. Preserving proprietor's data and information in cloud is one of the top most challenging missions for cloud provider. Many researches fanatical their valuable time's to discover some technique, algorithms and protocols to solve secrecy issue and develop a full-fledged cloud computing standard structure as a newest computing to all cloud users. Some researchers came forward with cryptography technique, cyber middle wear technique, noise injection and third party layer technique to preserve privacy about data in cloud. We propose a hybrid authentication technique as an end point lock. It is a composite model coupled with an algorithm for user's privacy preserving, which is likely to be Hash Diff Anomaly Detection and Prevention (HDAD). This algorithmic protocol acts intelligently as a privacy preserving model and technique to ensure the users data are kept more secretly and develop an endorsed trust on providers. We also explore the highest necessity to maintain the confidentiality of cloud user's data.

* Corresponding author.
E-mail addresses: pdchandramohan@gmail.com (D. Chandramohan), dsathian@gmail.com (D. Sathian), raja.guru42@gmail.com (D. Rajaguru), vengattaraman.t@gmail.com (T. Vengattaraman), dhavachelvan@gmail.com (P. Dhavachelvan).

Peer review under responsibility of Faculty of Computers and Information, Cairo University.

Production and hosting by Elsevier

1. Introduction

This research focuses on data privacy and its protection in ubiquitous environment. Similarly the present paper endures its literature study and came to know, in next very few years all electronic devices which are not computerized also going to connect in an environment. The advancement of pervasive and ubiquitous computing (PUc) embeds wireless sensors devices to all stand-alone appliances and framing a ubiquitous

http://dx.doi.org/10.1016/j.eij.2015.02.002

composite environment. (Home appliances like TV, Bathroom Taps, key chains, coffee mugs, computers, mixer Grinder, Mixie, lights, cars, homes, offices, cities, finally the human body).

Multi-agent system approach improves human experience and quality of life without precise knowledge of the causal communications and computing technologies. PUc is interconnected as pervasive network of smart devices that politely, separately collect data and process to convey information. This environment acclimatizes the allied context and activities in a global scenario. Globally privacy issues are highlighted and viewed as a difficult task to meet the right requirement.

The users do not have idea; in what ways the PUc environment can be abused by malicious attackers, who the attackers are going to be etc. Users may find that, they probably will not be limited to the computer hackers. It is an open research challenge and a research problem to design a PUc infrastructure with its complete usability, privacy and security. Usually in early days the researchers ignored this research, they felt it is not an easy task to satisfy both pros and cons at a time. Very few researches get into some of the privacy issues and proposed few valuable techniques. Traditionally ubiquitous environment has a combination of devices and systems. In the literature few authors proposed a framework and techniques to handle the privacy issue, uninterruptedly to preserve the user's confidential data stored in cloud environment.

One of the first requirements of small, ubiquitous devices is that they are inexpensive, low-power devices. No one wants to have to change the batteries in hundreds of devices every year. Peer networking also contributed as a whole to provide a controlled device. Cheap computers will need a source of cheap, inexpensive power and it will use low-power components. Mobility of computers is the focus of much current research. In the next decade, MIT expects their students to have portable, book-sized computers with wireless Internet access. The network needs to be in place to support mobile applications and devices. Currently, the Internet Protocol (IP) assumes that the location and connection of a computer remain fixed. One aspect of current research in mobile computing is that of Mobile-IP where IP is enhanced to allow a computer to roam and keep the same IP address. The Internet Engineering Task Force (IETF) maintains a Mobile-IP Web page to develop the standard. Basically, Mobile-IP works by assigning a Home agent on the permanent network for a computer. When the mobile computer (or the 'mobile host') moves from one network to another, it notifies its home agent of its new location. The home agent then intercepts and forwards packets destined for the mobile host.

Research is also being done in being able to move applications. Applications will need to move off of a workstation onto a tab, or perhaps the application will move with the user. Distributed web service monitoring process discussed in. Olivetti Research Laboratory has created the ORL Teleporting System to create mobile applications using the X Window system. A proxy X server routes the input and output of an X application to any X display. Research is also being done in the hardware necessary to create low-cost devices which can connect to the Internet.

The trend will be toward small, disposable computers. The MIT Media Laboratory is proposing a design of a network interface chip that would be small and inexpensive. It is called the Filament Chip. Weiser et al. envisions buying a six-pack of computers. These devices are meant to be practically invisible, and casually used. That means the user interfaces must be simple, apparent, and obvious. An awkward user interface could negate the whole purpose of the device. Ubiquitous computing forenames the third wield in computing, just currently beginning. First were mainframes, each shared by masses of people.

Now we are in the special computing age, individual and machine staring restlessly speaking at each other. Subsequently omnipresent or the epoch of serene tools in Fig. 1 shows the technology shift away from the background of daily lives. Mark Weiser is the father of ubiquitous computing. Ubiquitous computing is commonly the contrary of essential implicit realism. Virtual reality puts masses inside a computer spawn, ubiquitous computing services the computer to live away at this point in the human race. Virtual reality is mainly a mount authority dilemma and ubiquitous computing is a very tricky integration of soul factors, computer discipline, trade, and communal sciences.

This paper is organized with different sections as follows. In Section 2 the development process of secure infrastructure, secure service discovery, virtual objective convergence, privacy fortification and bio-metric authentication for pervasive and ubiquitous computing (PUc) is discussed. The user's insecure circumstance and risk factors of service requestors and providers security fame are monitored using hybrid hash authentication for anomaly service user's detection, are discussed in Section 3. In Section 4, the proposed system is summarized with a discussion under Section 4 and finally in Section 5 the work is concluded with future direction.

2. Backgrounds and development process of pervasive and ubiquitous computing

Computing arrive at an growing inclination of pervasive computing and ubiquitous computing with the hand-shake of

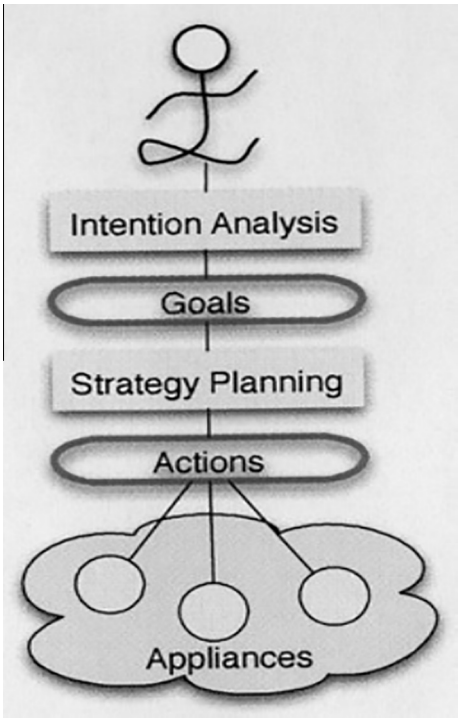

Fig. 1 Target based communication smart environments and self-organizing machine. Information retrieval IR-CM, bluetooth-CM, recommender-RS, lamp-LS, whiteboard-WBS, confidential-CFS.

microprocessor techniques to converse typical information geographically. The terminology pervasive and ubiquitous means presented universally. Pervasive computing devices are completely coupled and frequently available. Pervasive computing relies on the junction of wireless technologies, advanced electronics and the Internet. The goal of researchers working in pervasive computing is to create smart products that communicate discreetly. The products are coupled to the Internet and the data they generate are easily offered. An example of a practical application of pervasive computing is the substitute of old electric meters with elegant meters.

Mitrovi et al. [1] designed a system named Radigost using interoperability standards its main advantage is all agents can transparently interact with other agents in existing system or if there presents some third-party system it act as a multi-agent system to interact and fame the expected solution. Dhasarathan et al. [2], a petri-net privacy preserving framework in which acts as a multi-agent system to preserve the privacy of user by a cohesion technique which can handle multiple tasks. Afzali et al. [3], mobile nodes and static agents collaboratively acts as multi-agents with detector agents using an immune algorithm. Franco et al. [4], a coordination model is developed using nature-inspired approach called SAPERE. It synthesis the multifold requirements of modern and emerging pervasive services and it shows how it can affect the rest of other services.

Murugaiyan et al. [5], the need and hush–hush preventing cloud users' data by privacy preserving framework. It also describes the prevention of stored data and de-identifying unauthorized user attempts by maintaining a log monitoring for promoting allusion to providers and users. Pieters et al. [6], proposed a logic-based and graph-based approaches to formalize quantitative policies for security obligations to monitor the high performance computing systems. It is associated with quantitative analysis of external agents based on the time and adversary need of the process. Chandramohan et al. [7], a privacy policy is framed to allow the service requesters in a complex environment under limited privileges. A framework is designed as a test bed for evaluating the suitability and privacy of the service requester in a DWS environment and to emulate the realistic SOA environments.

Eldayem et al. [8], a security technique based on watermarking and encryption is proposed using Digital Imaging and Communications in Medicine (DICOM). Huffman compression algorithm is used for compression of images without the affecting the quality of original file. Khedr et al. [9], a hash-based security scheme for a simple, low cost and scalable security scheme relying on one-way hash functions and synchronized secret information. The scheme provides a two steps mutual authentication between the backend server and the tag. It follows the tag delegation and secures tag ownership transferring for a secure channel between the tag reader and the backend server to complete the authentication process.

Chandramohan et al. [10], an evolutionary model to maintain the integrity of original data stored in cloud provider region. To preserve valuable information Evolutionary model based privacy preserving in the cloud and develop trust among providers for maintaining the users confidentiality globally. Soliman et al. [11] evaluate and compare the most prominent anomaly-based IDS systems for hierarchical WSNs and identifying their strengths and weaknesses. Comparison is carried out using a set of critical evaluation metrics to ensure the performance and security and narrates in Fig. 1. Chandramohan et al. [12], an authenticated Key Exchange Protocol to maintain the user identity management and also a symmetric key encryption algorithm to minimize the computation cost and communication cost of service interpreters. Harshvardhan et al. [13], a dedicated hash function to ensure the privacy and preventing integrity of a message by MNF-256 based on the design principle of NewFORK-256.

Paul et al. [14], to improve the data availability and consistency in a network interconnection structure called the Distributed Spanning Tree (DST) has been employed. It converts the peer network into logical layered structure using GRM strategy and provides a hierarchical mechanism for replication management. chandramohan et al. [15], to develop the trust among cloud providers the service requests have to rely on few policies which are driven from providers by maintaining a high secrecy Hierarchical Petri-net based privacy nominal model for the Cloud. Jhih et al. [16] an authentication scheme is in need to show the perceived security threats scheme for an enhanced security key management. It is identified by an authentication scheme with key agreement based on the elliptic curve discrete logarithm problem.

Hao et al. [17] support the public verifiability without help of a third-party auditor, the proposed protocol does not leak any private information to third-party verifiers moreover it is verified through theoretical analysis. Wang et al. [18] EasiTia is a pervasive traffic information acquisition system which adapts a cross-correlation-based vehicle-detection algorithm and it is designed based on wireless sensors networks. Moreover it follows an cost-effective collaborative traffic information processing mechanism, Based on real road environment experimental analysis. Christos et al. [19], the exchange of information in mobile nodes is in an ad hoc networking to do collaborative context awareness for identical context processing. To withhold systems high performance maintenance, a fame of hierarchical information model with an information diffusion process is organized periodically.

Venkatesan et al. [20], a failure recovery model using K-response technique in which each and every host dispatching the agent and have the clone to recover the agents original state and report the agent status periodically. Deyi et al. [21], multi-way authentications to tighten the access control for sensitive data in clouds provider and users. It activates and enables single sign-on in the cloud by a trust-overlay network. Wang et al. [22], the least configurable computing resources guiding an cloud user to access their data remotely irrespective of the global infrastructure. The system also eliminates the physical control of storage region, its dependability and security. The nascent cloud economy becomes fully established in and around the public cloud data storage. Ubiquitous users computation resources also provide a transparent data access. Moreover, it is a cost-effective method for cloud information users. Zhang et al. [23], an identity-based cryptosystem to preserve and defense the original user to handle misbehavior in VANET access. Without compromising the data privacy and security system for VANETs is designed to achieve privacy desired vehicles.

Haodong et al. [24], a search engine named Snoogle is designed using an information retrieval technique and to reduce communication overhead it follows a bloom filter. It would find a particular mobile object located geographically and also it lists the objects that fit to users query. Moreover,

to preserve sensitive information preserving mechanisms have adopted. Zheng et al. [25], an algorithm is developed by weighted round-robin (WRR) and a greedy algorithm for aiming to maximize battery efficiency globally for the computer-assisted health-care systems. An efficient energy management system is designed for healthcare management. Taleb et al. [26], a Pervasive computing environment is more interrogating for an affective incarnation of sensor infrastructures with computing systems. Moreover, to identify and detect the periodic changes took place in patients, a high secret information preserving and sharing system is needed to inform and report the current states with the health-care management.

Vengattaraman et al. [27] software testing agent is constructed as a hybrid agent as a multi-agent testing attempt to validate the multi-agent system based on application perspective, with a regular working environment and exceptional working environment. Abirami et al. [28], a keyword based approaches used for retrieving information from document images are surveyed from the past researches on character based text extraction from document image retrieval. Huang et al. [29], a framework for cloud storage in order to maintain and preserve the users privacy an interactive protocol is designed. However, an extirpation-based key derivation algorithm is developed for the framework and evaluated with the lazy revocation, multi-tree structure and symmetric encryption algorithms for its performance. Vengattaraman et al. [30] an e-learning technique for the development of Information and Communication Technology (ICT) based on effort prediction. However it is observed from different perspectives of system, learner and teacher until the ground level of personalization in the e-learning environments fulfilling by providing domain specific contents.

Xiaodong et al. [31], in vehicular ad hoc networks, enabling a double-registration detection scheme and also a dynamic authentication technique as a privacy-preserving key management scheme called DIKE. Moreover, to achieve the session key's backward secrecy a dynamic threshold integrate technique is adapted in the traditional procedure. Amini et al. [32], a supervised and unsupervised time series analysis mixed method to capture the location of device and the position of sensor in human body. This technique ensures the accuracy in medical monitoring system. Chandramohan et al. [33], in the cloud storage area there is a need of high privacy in maintaining digital data. The service users and service a provider encloses a policy agreement based on the universal standard to prevent form decoding from third party intruders. Rao et al. [34], in the emerging Cloud storage the data protection is under screening. However, a policy of 'Divide and Rule' method is proposed to place data and keys separately on different clouds systems and accessed on request verification demand. It follows a double authentication and hybrid obfuscation technique it is multiple functionalities plug-in, adopted to minimize the loss of cloud user privacy and reduce the data lose.

Hajian et al. [35], a new privacy preserving clustering (PPC) technique is designed for data owners to share their sensitive information in a distributed environment. The composite use of Haar wavelet transforms (HWT) and scaling data perturbation (SDP) hyped for protecting private information globally using PPC. Liao et al. [36], web service toolkit is developed to improve the service reliability in a pervasive environment. Moreover, it is capable of integrating heterogeneous systems during autonomous composition, failure detection, and recovery of user query requests and responses. Chandramohan et al. [37], in order to preserve the confidential information a Hybrid authentication technique with limitations of access from intruders and preserves better utilization of user's confidential data by limiting the users authorization process.

Bondavalli et al. [38], a quantitative assessment of QoS is extracted from the abstraction and decomposition of holistic approach for developing a framework for managing the system complexity. A stochastic analytical modeling is encompassed for a complete end-to-end scenario. Weiser et al. [39], in ubiquitous environment the computational devices are invisible and their computing process is so complicated and uncontrollable stage. In such critical issue the users' private information prevention is at a high commendable risk. Abosamra et al. [40], mobile agents are introduced as Dynamic Source Routing for a secure communication in the wireless network. The performance of the system is improved with the symmetric key encryption/public key encryption technique. Wuquan et al. [41], graph topology is directed for interaction of agents and the leader is designed for a stochastic analysis for a distributed integrator system for validation of nonlinear multi-agent systems.

In the literature study electric meters had to be manually read by a company ambassador. Smart meters report usage in real-time over the Internet. The influence of company is an outage, reorganize thermostats according to the homeowner's commands, launch messages to demonstrate units in the domicile and regularize them. The word ubiquitous can be defined as existing or being everywhere at the same time, persistently meet, and extensive. Privacy and security technically the term ubiquitous technology is everywhere and we utilize it the entire instance and in Fig. 2, it indicates the popularity of these technologies to use them without trust propos tool form the. We focus on the assignment at hand, making the technology successfully invisible to the user. Ubiquitous technology is repeatedly wireless, mobile networked creation to its users further connected to the world around and the people in it.

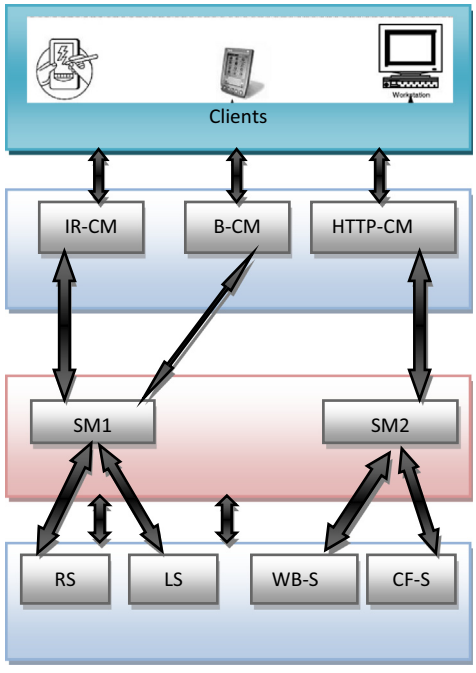

Fig. 2 Privacy centaurs classification mechanism.

Table 1 Ubiquitous and Pervasive Computing Performance metrics, its features, complexity and limitations.

Author and Year	Context in use	Ubiquitous and Pervasive Performance metrics	Metrics features	Complexity	Performance and Limitations
Wang et al. [24]	By evaluating some cyber corporeal system platforms and systems that have been residential recently, including health care, routing, salvage, smart transportation, social networking, and gaming applications	Through these reviews, we hope to demonstrate how CCS applications utilize the corporeal information unruffled by wireless sensor networks to bridge real and cyber space's and identifies significant research challenges related to CCS designs	A CCS application may bridge numerous isolated WSNs and take actuation dealings. We have seen a lot of flourishing vehicle- and mobile phone-based CCS services	Data from such applications are also estimated to be uninterrupted streaming data at a very large volume, storing, dispensation, and interpreting these data in a real-time comportment is critical	Through these reviews, we hope it will help to motivate more scientific development and evolution for future CCS applications
Zheng et al. [25]	Anticipated a bio metric based interior finger printing with assorted clients and service contributor	Mapping-based solutions have been obtainable that require manual and error-prone calibration for each new client. Present's hyperbolic locality finger printing, to record finger prints as signal vigor ratios between pairs of base stations as an alternative of unlimited signal strong point values	A routine mapping-based method that evades calibration by learning from on line capacity. The obtainable solutions decipher the signal strength client difference problem without requiring further physical calibration	The assessment shows that the elucidation can address the signal power heterogeneity problem without requiring extra physical calibration	The anticipated loom referred more data to estimate if they are citation such as always use a client which maximizes the number of unhurried base stations can address the hitch
Taleb et al. [26]	Advances are to do the need to trust any party such as a mediator server or peers with their position and uniqueness. CCS application may bridge numerous isolated WSNs and take actuation dealings. We have seen a lot of flourishing vehicle- and mobile phone-based CCS services	A proficient algorithms for users to partition a k-anonymous imprecise location and to arbitrarily select one of peers with unvarying possibility who forwards the service demand on behalf of the user	Proposed by evaluating some cyber corporeal system platforms and systems that have been residential recently, including health care, routing, salvage, smart transportation, social networking, and gaming applications	Through these reviews, we hope to demonstrate how CCS applications utilize the corporeal information unruffled by wireless sensor networks to bridge real and cyber space's and identifies significant research challenges related to CCS designs	Data from such applications is also estimated to be uninterrupted streaming data at a very large volume, storing, dispensation, and interpreting these data in a real-time comportment is critical. Through these reviews, we hope it will help to motivate more scientific development and evolution for future CCS applications
Hao et al. [17]	Information flows from the corporeal to the cyber world and vice versa acclimatizes the congregate world to human behavior and social dynamics. Research issues and confront from a worldwide standpoint	Cyber world collective features Comprehensive situation-awareness top down vs bottom up, the authority of the stacks, Decentralized power, Diversity and resolvability and mechanisms design	The main dispute confers in represents a notable, but not extensive, list of explore opportunities cause by the cipher convergence. Many others follow a line of investigation challenges in the same and identified it as a difficult task	Urban/participatory sensing techniques have a major role in understanding both the physical and the virtual world. Understands and characterizes the inter-relation between real-world social structures and online social networks for data dissemination in the cyber–physical world	New paradigms for location purpose in the replicated–objective world, Privacy issues in participatory sensing of the cyber–material, in addition they demarcate the need for agree to concern connected to autonomic performance, opportunistic network and computing, and quality of information

(*continued on next page*)

Table 1 (*continued*)

Author and Year	Context in use	Ubiquitous and Pervasive Performance metrics	Metrics features	Complexity	Performance and Limitations
Amini et al. [32]	The proposed system came out with a model for a confidence and secure service discovery in Pervasive and ubiquitous computing location	The use of intricate algorithms and potent infrastructure is infeasible due to the unstable character of pervasive environment and petite pervasive devices	The representation is a hybrid one that allows both locked and unlocked contraption of services. It allows service sighting and distribution based on communal trust. The privacy prevention model holds the announcement and service allocation security issues	It also integrates a confidence mode for distribution services with unidentified devices. Researchers designed an undemanding and efficient model that inherits secrecy related issues without causing much battery power consumption	By realize a fusion mode of procedure the potential research can diminish the overhead of encrypting messages each time a device requests or provides services
Wang et al. [18]	Proposed work securely permits customers to access and utilize services in various networks. He presents a service register and invention mechanism implemented through a ladder of examining its management	The proposed system is executed using Java and XML as the exclusive standard for interactions and information swapping	The scheme built upon a short Public Key relation that provides validation, non-refutation, anti-playback, and access power. Elegant cards are worn as protected for digital record	The elastic illustration of confidence in sequence and offered its accomplishment scheme and describes his variation to propose a disseminated conviction. His accomplishment is relevant to any circulated examine transportation like agitated, itinerant, or ad hoc, etc	The practice of creating services available to an expansive continuum of users demand and addition of sanctuary architecture. Services with susceptible for utilization and mistreat them during its access is not effectively administrated
Anagnostopoulos et al. [19] [2011]	Cheap computers will need a source of cheap, inexpensive power and d will use low-power components. Mobility of computers is the focus of much current research	The network needs to be in place to support mobile applications and devices	In the next decade, MIT expects their students to have portable, book-sized computers with wireless Internet access	One aspect of current research in mobile computing is that of Mobile-IP where IP is enhanced to allows a computer to roam and keep the same IP address	Currently, the Internet Protocol (IP) assumes that the location and connection of a computer remains fixed
Bondavalli et al. [38]	The Internet Engineering Task Force maintains a Mobile-IP Web page to develop the standard	It notifies its home agent of its new location	Mobile-IP works by assigning a Home agent on the permanent network for a computer	The home agent then intercepts and forwards packets destined for the mobile host	When the mobile computer (or the 'mobile host') moves from one network to another
Liao et al. [36]	Toward Reliable Service Management in Message-Oriented Pervasive Systems	As mentioned in the introduction, privacy issues are necessarily not technical. As ubiquitous policy saturate the every-day lives of regular citizens, our privacy protection procedures will have mounting impact on their lives	In this paper a systematic scrutinized of privacy issues in ubiquitous and pervasive computing	It is important that study of privacy fortification tolerate in mind what must be protected	To identify key functionalities and services of PUc, reference malicious attack managing practice from the organized viewpoint and programming Ubiquitous application notion, services and runtime support. We have promoted these into several sub-viewpoints

2.1. Approaching methods for a secure infrastructure for PUc environment

Different approaches for maintaining privacy in PUc-(pervasive and ubiquitous environment). Wang et al. proposed his work securely permit customers to access and utilize services in various networks. He presents a service register and invention mechanism implemented through a ladder of examining its management. The scheme built upon a short Public Key relation that provides validation, non-refutation, anti-playback, and access power. Elegant cards are worn as protected for digital record. The proposed system is executed using Java and XML as the exclusive standard for interactions and information swapping.

He developed an elastic illustration of confidence in sequence and offered its accomplishment scheme and describes his variation to propose a disseminated conviction. His accomplishment is relevant to any circulated examine transportation like agitated, itinerant, or ad hoc, etc. His future looms to focus on the practice of creating services available to an expanded continuum of users demand and addition of sanctuary architecture. Moreover, the architecture servers the requested service with appropriate services with susceptible for utilization and mistreat them effectively administrated by controlling the user access to confidential information.

2.2. A secure service discovery in PUc

The scenery of ad hoc networks service discovery representation is needed for tenacity safety and privacy issues with simple solutions. Navid Amini et al. describe a model for a confidential and secure service discovery in Pervasive and ubiquitous computing location. The use of intricate algorithms and potent infrastructure is infeasible due to the unstable character of pervasive environment and petite pervasive devices. His representation is a hybrid one that allows both locked and unlocked contraption of services. It allows service sighting and distribution based on communal trust.

The privacy prevention model holds the announcement and service allocation security issues. It also integrates a confidence mode for distribution services with unidentified devices. Researchers designed an undemanding and efficient model that inherits secrecy related issues without causing much battery power consumption. By realize a fusion mode of procedure the potential research can diminish the overhead of encrypting messages each time a device requests or provides services. This model can be extended to facilitate multi-hop discovery and service sharing and by including features like dynamic service integration.

The author proposed a test bed for evaluating the efficiency of services by filtering its functional and nonfunctional QOS-(Quality of Services) parameters. By mathematical evaluation the QOS parameters are verified for service efficiency. The proposed approach concludes by deriving parameters and their function for evaluation, one can prove the efficiency, precautions and recital of service. By adopting these features in PUc we can derive our own parameters and functions for maintaining privacy and security in all ubiquitous computing environments.

2.3. Dispute and prospect in the era of virtual-objective convergence

Main challenge in this expertise situation real-world apparatus intermingle with cyberspace via sensing, computing and communication elements, thus motivating toward what is called the Cyber substantial humanity convergence. Zhuo Hao et al., Information flows from the corporeal to the cyber world and vice versa acclimatize the congregate world of human behavior and social dynamics. Research issues and confront from a worldwide standpoint. Cyber world collective features Comprehensive situation-awareness top down vs bottom up, the authority of the stacks,

Decentralized power, diversity, resolvability and mechanisms design are the main dispute confers in represents a notable, but not extensive, list of explore opportunities cause by the cyber convergence. Many others follow a line of investigation challenges in the same and identified it as a difficult task. In urban/participatory sensing techniques, a major role in understanding both the physical and the virtual world scenario described as a ubiquitous environment. Understands and characterizes the inter-relation between real-world social structures and online social networks for data dissemination in the cyber–physical world. New paradigms for location purpose in the replicated–objective world, Privacy issues in participatory sensing of the cyber–material, in addition they demarcate the need for agree to concern connected to autonomic performance, opportunistic network and computing, and quality of information (see Table 1).

2.4. Privacy fortification for location-based services and Cyber Corporeal Systems (CCS)

The advance approach of user information maintenance by Taleb et al. [27] is to improve the trust of third party such as a mediator server or peers with their position and uniqueness. The author proposes proficient algorithms for users to partition a k-anonymous imprecise location and to arbitrarily select one of peers with unvarying possibility who forwards the service demand on behalf of the user. Wang et al. [25] proposed by evaluating some cyber corporeal system (CCS) platforms and systems that have been residential recently, including health care, routing, salvage, smart transportation, social networking, and gaming applications. Through these reviews, we hope to demonstrate how CCS applications utilize the corporeal information unruffled by wireless sensor networks to bridge real and cyber space's and identifies significant research challenges related to CCS designs.

A CCS application may bridge numerous isolated WSNs and take actuation dealings. There presents a lot of flourishing vehicle and mobile phone-based CCS services. Data from such applications are also estimated to be uninterrupted streaming data at a very large volume, storing, dispensation and interpreting these data in a real-time comportment is critical. Through these reviews, we hope it will help to motivate the more scientific development and evolution for future CCS applications.

2.5. Biometric privacy and security

In due course the anticipation of information technology development era via bio metric based interior finger printing proposed by Nenggan Zheng et al. intaglios. Mapping-based solutions have been obtainable that require manual and error-prone calibration for each new client. Present's hyperbolic locality finger printing, to record finger prints as signal vigor ratios between pairs of base stations as an alternative of unlimited signal strong

point values. He presents a routine mapping-based method that evades calibration by learning from on line capacity.

The assessment shows that the elucidation can address the signal power heterogeneity problem without requiring extra physical calibration. The obtainable solutions decipher the signal strength client difference problem without requiring further physical calibration. The anticipated loom referred more data to estimate if they are citation such as always use a client which maximizes the number of unhurried base stations can address the hitch.

3. Work package and proposed approach

In this paper for defining the ubiquitous computing environments as erudition environments in which all students have access to a diversity of digital devices and services. Moreover, it includes the PC associated to internet and also mobile computing devices. If at all found at anytime and anyplace a service is in need by using ubiquitous computing. Moreover the definition of ubiquitous computing holds the idea of both teachers and students are active accomplice in the learning process, who critically scrutinize information create new knowledge in a variety of ways communicate what they have learned and choose which tools are appropriate for a particular task.

Omnipresent is a computing which changes every day activities in a variety of ways. Usually in today's digital tools consumer has a tendency to multiple tasks from their door step. The user's sustainable activities correspond in different behavior and may depend on the device operated globally. (Be more energetic, Visualize and use objective and chronological spaces differently, Have more control, Worldwide and restricted, Social and individual, Public and private, Invisible and visible, An aspect of both information establishment and propagation).

The enormous development in cloud and its Data's storage in it are accessible to users in the form of different services with the help of traditional networks and it is also know to be cloud storage. In which it holds a brief description about cloud users profile, business details and back up information to make available ubiquitously via internet as backbone. Online data backup, data archiving, data compliances, disaster recovery, compliance regulations are some of the issues in cloud portability. Many technologies have been developed for cloud portability based on cloud provider's service level agreements.

In information portability, the suitable data is stored in the form of Cloud backup and provided on demand as a service to the requested user. The proposed system would ensure the data security, privacy, and data recovery without disturbing the original bandwidth communication and related issues. To reduce user information management cloud providing companies are farmouting their customers information to cloud back up service providers as an infrastructure and power maintenance. Some nominal metrics are adopted to identify the maximum possibility of storing information. There may be many risk factors evaluated along with this as a data offsite replication and data disaster recovery as a security issue for both providers and consumers. At administration level the need for cloud storage has been adopted in several principles to serve their clients on demand at all circumstances with high privacy and security. Cloud Providers follow many encryption techniques to breach intruders who are hijacking others information without any prior intimation.

There must be high concern about location based services to identify those intruders from their access point 50–70% information hijacked during communication, in mean while more power also consumed at the same time. Privacy law and policy may vary from country to country and cloud providers too. Some complicated law has been in practice to avoid violation of confidential information explored out of their nation as well as organization. Privacy laws are framed as per company normality and stockholders suggestions. In past few years, cloud computing has grown a gifted trade model as highest growing profitable and IT industry. Now, recession-hit companies are increasingly realizing that simply by tapping into the cloud they can gain fast access to best-of-breed business applications or drastically boost their infrastructure resources, all at negligible cost.

But as more and more information on individuals and companies is placed in the cloud, concerns are beginning to grow about just how safe an environment is? Breached security and privacy system adopted in cloud organizations and their personals make them comfort with the public and control over their information in cloud by controlling the users information with the help of encryption and decryption technique in limited portable devices as a preventive measure to block few info from attackers. Hardware supported VLSI circuit it gets varied accordingly as per company rules and their upgraded tools which they are using for these purpose.

3.1. Users risks in cloud computing

Cloud computing may have many undeserved risk factors and it will get reflected over company both economically and customer wise in their overall profit in this most complicated cloud business world. As a measure of losing their own customers out of their control the cloud providers framing ACT and privacy principles to violate the unnecessary losing of information of their users.

3.2. Security approach fame by cloud hosting providers

Cloud providers have their own flexibility while framing their privacy laws and may get varied between companies even it is directly propositional to the national law and order schemes it also differs as per the country violations. It is mainly due to initiation of information leverage of customers who are doing some illegal activities against one nation internal security and maintain their military and other secrecy about them to bordering nations and so on. Author proposed a novel framework and technique to handle the privacy issue, uninterruptedly to preserve the users confidential data stored in cloud environment.

If a cloud user willing to switchover from one provider to another first the provider should ensure all his historical reference and in Fig. 3 e-discovery backups are get completely removed from the source and get inserted or stored in another cloud provider whom the clients want to have his data or information here cloud archiving and aggregation play an important role to give surety to both providers and users. The archiving will chose the best provider based on their back up storage and its mining information. During integration the main and real portability issue will be hitting peak for all CP-cloud providers.

Some CPs chosen limited service level agreements as a safety measures to hold their clients with them. All these portability issues combined together and make a question mark for future cloud storage and cloud computing itself. Still it is a research issue

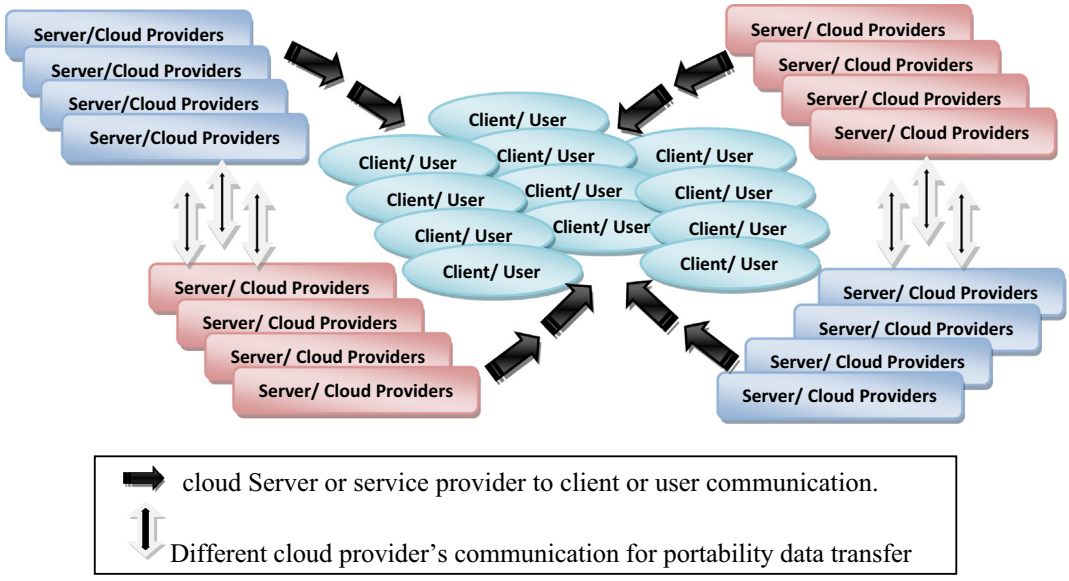

Fig. 3 Data arbitrary block to provide interactive client identification and authentication.

one cannot enjoy full-fledged cloud computing benefits until otherwise a strong SLA agreement or global standard framed to resolve these issues. A hybrid authentication technique has a milestone for solving the portability issues in cloud service. In this paper an end point lock approach is highlighted by detecting the anomaly operations and providing hash authentication coupled with Diff–Hallman exchange protocol together as a hybrid model.

3.3. Hybrid authentication technique end points lock for cloud

We are going to propose a hybrid authentication protocol for cloud architecture layer (AaaS/SaaS) with the composition Hash Diff Anomaly Detection (HDAD), privacy prevention algorithm as a protocol. If the index searched and identified as an unauthorized access among cloud users it will hijack the user account and trace who what it. If (Sx = CDS)

$$Sx = \mathrm{CDS}_i(X_i)\mathrm{CDS}_i(X_i)\cdots\mathrm{CDS}_i(X_i) \tag{1}$$

It is noted that it was not particularly important to the service requests about someone data as an unknown user for the requested query. Thereby, typical search $S(x)$ was irrelevant retrieval, or that can be counted using Restricted Data access (Rda). It is identified the actual relation to $S(x)$ and CDS($X_1 \ldots n$) and it can be characterized as

$Si : N \to K$, where $1 \leqslant i \leqslant n$

$$S(x) = \sum \mathrm{CDS}_1(X_1)\mathrm{CDS}_2(X_2)\cdots\mathrm{CDS}_n(X_k), \tag{2}$$

$$S_x = \mathrm{CDS}_1(X_1), \mathrm{CDS}_2(X_2)\cdots\mathrm{CDS}_n(\mathrm{CDS}_k) \tag{3}$$

The same request will be process until the unauthorized user get his information, as an avoidance we are going to calculate the trigger by means of number of request and its repetitions to the same data while it get expatriate it is denoted and identified by using,

$$S\_X(x) = \sum\nolimits_{-}(n = k) \wedge \infty C(n,k)x \wedge n/n! = [-\ln(1-x] \wedge k/k! \tag{4}$$

$Sx \to$ search infinite date, CDS – cloud data storage.

- Hash based authentication technique.
- Anomaly Detection interface algorithm.
- Diff–Hallman exchange Protocol.

PBEB-Privacy Breach End Point before Information hijacking (IH), Hybrid Privacy Preserving Hash Diff Anomaly Detection and Prevention algorithm.

Hash Diff Anomaly Detection and Prevention Algorithm (HDAD)

Begin
do SR where SR = 1 then,
$ND_i = \{x_i(d), 0\}_{i=1}^{k-N}$;
$SD_i = \{x_j(d)\}_{j=1}^{m}$;
$SSD_i = \{x_t(d), 1\}_{t=1}^{N}$
Do, ND_i, SD_i and SSD_i might be frequent service requesters,
Go to step 1: until SR → End; otherwise
Follow: check point SD_i and SSD_i triggers 'i';
M_A is performed by an collaborative task of SA, USA and SSA
$M_A = \{S_A + US_A + SS_A\}_{i=1}^{k}$ *(∵ $k \leqslant m$);*
$US_A \leftarrow \prod_{r=i}^{t} S_r$ *(∵ $r = n$ x m, ∵ $n \leqslant m$);*
D_o *– Search for ND_i;*
If SR → ND_i found unknown then
$S_A \to D_o \to ND_i$;
$US_A \to D_o \to ND_i$;
$SS_A \to D_o \to ND_i$; *(∵ $i = n$-k)*
Endif;
Evaluating the detection process
$PCV_i \to SL_i \to EV_i \to V_i \to P_i$;
$PCV_i \leftarrow \prod_{i=1}^{k}\{SL_i, EV_i, V_i, P_i\}_{i=1}^{k}$;
$M_A \leftarrow \prod_{i=1}^{k}[I_D\{S_A + US_A + SS_A\}_{i=1}^{k}]$; *(∵ $k \leqslant m$);*
$HID \leftarrow PCV_i \leftarrow M_A$;
Repeat: Until D_o, $SR \neq \phi$;
End;

Notations Used:
D_o-Data Observed, SR-Service Request, X_i-Services, ND_i-Normal Data, SD_i-Unsupervised, SSD_i-Semi-supervised, t-Temp, d-data, N = Normal data, m-intermediate, PCV_i-Possibility Checking and Verifying, EV_i-Evaluating, V_i-Validating, P_i-Performance, M_A-Multi-agent, S_A-Supervised agent, US_A-Unsupervised agent and SS_A-Semi-Supervised agent, SL-Study and Learn, HID-Host Identification.

Unsupervised anomaly detection	Supervised anomaly detection	Semi-Supervised anomaly detection
A	-	10
B	A	10
C	A	8
D	B	10
E	A	18
F	D, E	10

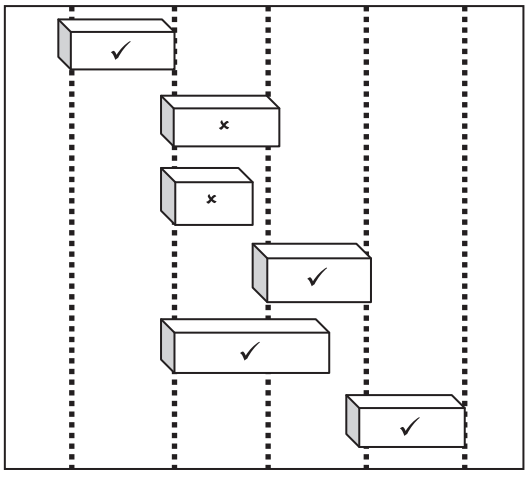

Fig. 4 Identification of intruders using Hash Diff Anomaly Detection and Prevention (HDAD).

To identify the unknown and abnormal user request a multi-agent (M_A) approach is followed with the collaboration task of intelligent agents (S_A-Supervised agent, US_A-Unsupervised agent and SS_A-Semi-Supervised agent). Data observation Do is processed in accordance with the agents. M_A will check the SR and its Reachability to the data storage area (DSA). Each stage of agents is reported to the system and it is recorded periodically. Error logs and SR attempts are updated on regular basics to identify the HID system.

3.4. Hash based authentication technique

It is a cryptographic technique to encrypt a message authentication code with combination of secret key e.g. (Opad-Otter padding and ipad-inner padding) service provider who wish to authenticate the user and particular provider's server and giving right authority. The hash based authentication interacts with users and cloud providers with an interactive identification technique, this technique get varied as per the authorization level and authentication stages.

The overall work flow and its internal flow explained in Fig. 3 with the help of the proposed hybrid authentication technique. The un-known user's interposition could be identified and its critical path get pin pointed using the algorithm. Its internal process explained in Fig. 4. Its critical identification is handled more causational and necessary steps have been taken based on hiding and permitting access to the users to manage their data kept inside the storage area.

A-Authenticated, R-Response based on activity, O-Obligation due to critical infection Table 2 illustrates the authentication possibilities and its preconditions as per our proposed hybrid algorithm it will initiates the level of authorization as mentioned in the above table based on the validation steps presets in activity column. Each activity checked and verified for all possible critical section and finally it replied to the provider to permit or reject, from the notations we introduced inside the tabulated fields like (A, O, R) denote the different activity levels for an identification to providers. From those results the providers can easily took decision which user have critical identification to get inside the storage area for hijacking the secret data.

A esteem for sample information tested in a case processing illustrated in Table 3 and shown in Fig. 5 for data processing assimilation.

3.5. Anomaly detection interface algorithm (intrusion detection, unexpected activities in normal behavior)

The homogeneous data are usually identified but in some cases it cannot be identified as normal data in those cinereous these anomaly detection came into rule as fraud identification in a network that trying to insert in as an intruder, some more identification factors are there which may be so hard to identify, so we are considering ADI (Anomaly Detection interface) as a module for our proposal to identify the intruders who are trying to access the information as an unauthenticated users. Unsupervised anomaly detection agent, Supervised anomaly detection agent, Semi-Supervised anomaly detection agent and few techniques for anomaly detection are distance based techniques like (k-nearest neighbor, Local Outlier Factor), One class Super vector mechanism, Replicator (Neural network).

The inference of privacy breach identification by an intelligent multi-agent in a ubiquitous environment is observed and tabulated in Table 4 simultaneously it is plotted as shown in Figs. 6 and 7. The generated hash values are used to compute another message with the same hash values. There should be some defy attacks (finding any message with the same hash value) it is usually assumed that the hash function is public and not keyed with traditional CRCs. If it does not satisfy the predefined length which is large enough to resist those attacks normally in a 64-bit data since current advancement not meeting the stipulated size, now the sizes are considered

Table 2 Illustration of data portability activity and responsibility of various services.

Activity	Distance based technique	One class Super vector mechanism replicator	Cluster analysis based outlier detection	Secrete key cryptography	Key agreement protocol	Symmetric key cipher technique	⋮
Requirements	✓	×	✓	✓	✓	✓	…
Objectives	✓	✓	×	✓	×	✓	…
Specifications	×	✓	✓	×	✓	✓	…
High-level design	✓	✓	✓	✓	✓	✓	…
Publication content plans	✓	✓	✓	✓	✓	✓	…
Unit test plan	–	✓	✓	–	–	✓	…
Function test plan	–	✓	×	–	–	×	…
Component test plan	✓	×	✓	✓	✓	×	…
System Test plan	✓	×	✓	×	×	✓	…
Low-level design	–	✓	–	–	✓	×	…
Code	–	✓	–	✓	–	×	…
Unit test	✓	✓	✓	–	–	✓	…
Function test	–	✓	×	×	–	✓	…
Component test	✓	✓	✓	–	–	✓	…
First-draft publications	✓	✓	×	✓	✓	✓	…
System test	×	×	×	×	✓	✓	…
Second-draft publications	×	×	×	×	✓	✓	…
Regression test	–	×	✓	×	–	✓	…
…	…	…	…	…	…	…	…

Table 3 Case processing assimilation.

Case processing		N	Percent (%)
Sample	Training	293	68.6
	Testing	134	31.4
Valid		427	100.0
Excluded		4	
Total		431	

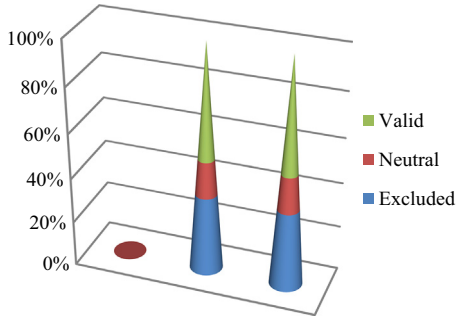

Fig. 5 User data processing assimilation.

Table 4 Privacy Breach identification process in pervasive environment by HDAD intelligent agent system.

Substring	Frequency (in%)	Frequency in run up
T	5.7971	24
Y	5.5556	23
F	5.314	22
N	5.314	22
A	4.8309	20
H	4.5894	19
B	4.3478	18
P	4.3478	18
Q	4.3478	18
Z	4.3478	18
E	4.1063	17
G	4.1063	17
K	4.1063	17
J	3.8647	16
W	3.8647	16
D	3.6232	15
U	3.6232	15
L	2.8986	12
R	2.8986	12
I	2.657	11
M	2.657	11
O	2.657	11
V	2.657	11
X	2.657	11
C	2.4155	10
S	2.4155	10

as too small and migrated to next level bit size 128–512 for the proposed system.

Hybrid Hashing functions are used to condense an uninformed length communication data to a rigid size, generally for consequent signature by a digital signature algorithm, by using our proposed cryptographic hash function. 'h' should satisfy some conditions. The HDAD agent identifies the intruders and its critical path responsibility matrix is represented in Fig. 8.

"h" Should obliterate all independent structures in the proposed algorithm public key cryptosystem (be unable to work out hash value of two different request messages are collectively given and their individual hash values are calculated) format. Moreover, "h" should be manipulated on entire message and it is noted as a one-way function, so that messages are

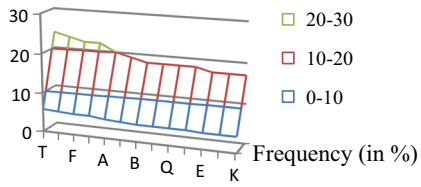

Fig. 6 Agent inference of privacy breach identification.

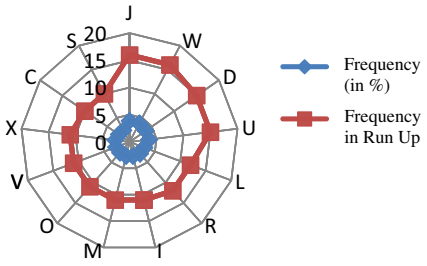

Fig. 7 Privacy breach identification in ubiquitous computing.

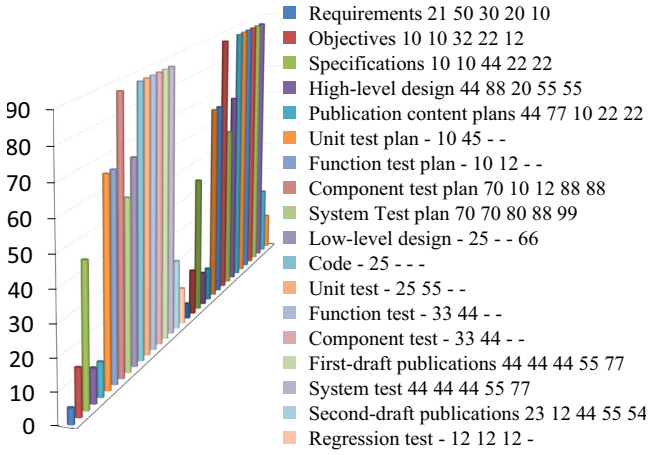

Fig. 8 Responsibility matrix representation and identification of intruders using critical path process HDAD.

Table 5 Collision monitoring by Hash Diff Anomaly Detection and Prevention (HDAD).

Run no.	Steps until collision	Check of the collision	Total steps
1	492	432	924
2	122	109	231
3	384	232	616
4	277	51	328
5	338	288	626
6	489	365	854
7	104	57	161

not disclosed by their signatures and also computationally infeasible with the given message.

3.6. Unique identifier (UID)

A unique identifier (UID) is a numeric or alphanumeric string that is associated with a single entity within a given system, as an identification factor exploit and expressed in proposed hybrid algorithm.

3.7. OAuth (OA)

OAuth (Open Authorization) is an open protocol for token-based authentication and authorization on the data storage area. OAuth allows an end users' account information to be utilized more secretly by the particular users only.

Calculating time: 0 year(s), 0 days(s), 0 h(s), 0 min(s) und 0.29 s(s). Steps required Hash operations performed. In improving the mitigation of privacy risk factors by coordinated approach with the identification of users and minimizing the collision of data from storage area whenever a communication took places. It may reduce the secrecy breach. Moreover, it is verified with certain number of runs and corresponding collision check is notified. The differences in data breach levels are identified and tabulated in Table 5 and its collision neutralization is shown in Fig. 9.

Tables 6 and 7 illustrate the anomaly detection and identification under normal service request and different service

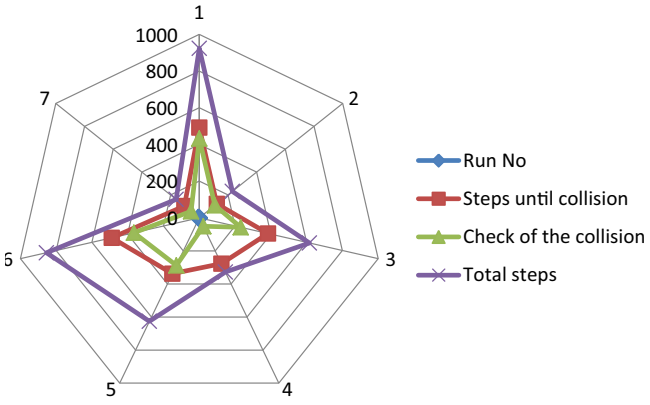

Fig. 9 Hash Diff Anomaly Detection and Prevention (HDAD) privacy collision minimization.

Table 6 Identified anomaly service attempts during normal processing in pervasive computing (ms).

Service requests	S1	S2	S3	S4	S5	S6	S7
Education server	2	5	6	3	2	6	5
Entertainment server	5	4	2	8	3	7	9
Financial server	3	5	4	3	5	8	8
Sports server	2	3	5	4	2	3	5
Forum server	6	2	3	5	2	3	2

Table 7 Anomaly detection and identified during average service requests.

Service requests	S1	S2	S3	S4	S5	S6	S7
Education server	0	1	2	3	4	5	6
Entertainment server	1	2	3	4	5	6	7
Financial server	2	3	4	5	6	7	8
Sports server	3	4	5	6	7	8	9
Forum server	4	5	6	7	8	9	10

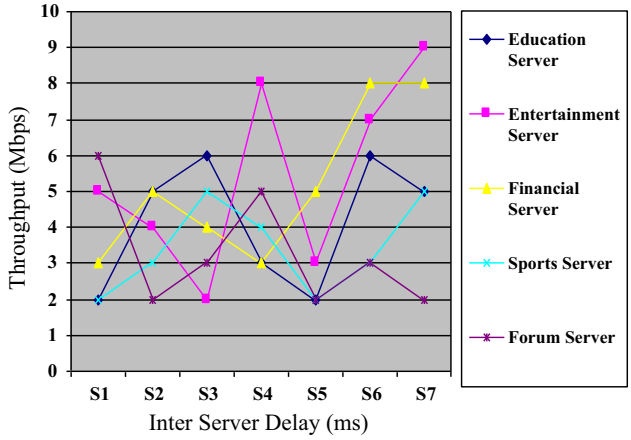

Fig. 10 Anomaly service attempts during normal processing.

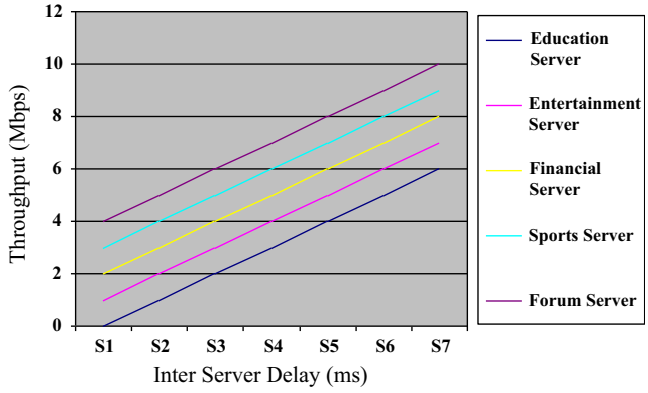

Fig. 11 Anomaly detection and identified during average service requests.

attempts with respect to ms and its corresponding throughput responses are noticed and recorded in log file. Similarly the notified results are plotted in Figs. 10 and 11 respectively.

Hash based authentication technique-HBAT, Anomaly Detection interface algorithm-ADIT, Diff–Hallman exchange Protocol-DHEP, S-Service. In Tables 8-10 illustrate the performance factors and the deviations are identified by comparing the proposed HDAD with relatively equalized systems. The outcome of the process is recorded with a high demand of anomaly attempts and its detection stages under HDAD comparatively showing good response.

4. Discussion

The researchers, academicians and practitioners studied the need and advancement in pervasive and ubiquitous device development and noticed the issue relating to personal information disclosure to unauthorized users. Privacy preserving of a user, they may be directly connected with pervasive devices in a ubiquitous environment. It is identified the issue pertaining to confidential information preserving is a leading and a must for the information technological advancement as identified from Tables 4 and 5 and its corresponding table illustrated by context in use.

As Ubiquitous and Pervasive Performance metrics, Advantages, Complexity, Performance and Limitations are listed eventually. From the table it is stipulated and coerce for privacy and security in pervasive and ubiquitous computing is an active research area, robustly driven by internal uniqueness of ubiquitous computing. It makes ubiquitous computing applications adaptive to the budding perspectives and to be intelligently personalized to user preferences. As mentioned in the introduction, privacy issues are necessarily not technical.

As ubiquitous policy saturates the every-day lives of regular citizens, the proposed privacy protection procedures may have mounting impact on their lives. It is important that study of privacy fortification tolerate in mind what must be protected. In this paper, we have systematically scrutinized privacy issues in ubiquitous and pervasive computing. To identify key functionalities and services of PUc have proposed a reference malicious attack managing practice from the organized viewpoint programming Ubiquitous application notion, services and runtime support. In this work privacy issues are promoted into several sub-viewpoints enormously it extorts functionalities from services as modeling, preprocessing, elucidation, capriciousness and illuminating and decisions.

It is an overview of the state-of-the-art of existing privacy techniques proposed by earlier author's effort in. This paper dealt with an ample privacy preserving techniques for

Table 8 Hash Diff Anomaly Detection and Prevention (HDAD) evaluation and its Consequence.

Anomaly identification tested service	Hotel service	Emergency health service	Booking service	Narration
Response time (ms)	10	10	10	✓
Service availability	Yes	Yes	Yes	✓
Reliability	Yes	Yes	Yes	✓

Table 9 Hash Diff Anomaly Detection and Prevention (HDAD) under different scenario validation.

HDAD anomaly detections with different conditions	Hotel service	Emergency service	Booking service
Passed	✓	✓	✓
Skipped	✓	✓	✓
Failed	×	×	×
Tested	✓	✓	✓

Table 10 HDAD overall performance evaluation process.

	Service provider 1				Service provider 2				Service provider 3			
	HBAT	ADIT	DHEP	HDAD	HBAT	ADIT	DHEP	HDAD	HBAT	ADIT	DHEP	HDAD
S_Request (ms)	6 ms	5 ms	8 ms	3 ms	4 ms	6 ms	6 ms	2 ms	9 ms	4 ms	8 ms	6 ms
S_Verification (ms)	5 ms	7 ms	5 ms	5 ms	3 ms	5ms	10 ms	4 ms	6 ms	9 ms	5 ms	4 ms
S_Validation (ms)	9 ms	6 ms	8 ms	5 ms	6 ms	9 ms	9 ms	5 ms	10 ms	5 ms	8 ms	6 ms
S_Waiting time (ms)	7 ms	10 ms	8 ms	7 ms	8 ms	6 ms	7 ms	4 ms	9 ms	12 ms	8 ms	7 ms
S_Response time	✓	×	49 ms	10 ms	✓	×	×	10 ms	✓	×	67 ms	10 ms
Service availability	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
S_Reliability	✓	×	✓	✓	✓	×	✓	✓	✓	✓	×	✓
Service passed	✓	✓	✓	✓	✓	✓	✓	✓	✓	×	✓	✓
Service skipped	×	✓	×	Dynamic	✓	×	×	Dynamic	✓	×	✓	Dynamic
Request failer (%)	23	26	10	7	17	13	8	5	15	17	11	6.8
S_Auto-recovery	Normal	Typical	Normal	Automatic	Normal	Typical	Normal	Automatic	Normal	Typical	Normal	Automatic

pervasive and ubiquitous environment, which is a challenging research problem yet to fine-tune in the current technological era. It also explores future research by focusing on solving personal information disclosure and preserving the privacy of ubiquitous device users and resolving it as earliest and most preferable in a tolerable and efficient approach.

Privacy breaching is everywhere in current technological computing and communication. This paper exhibits the necessity of upcoming computing privacy risks and corresponding preventing measures for a pervasive and ubiquitous based environment. Pervasive and ubiquitous computing (PUc) should become a reality in real time human lives environment. PUc users expect to access resources and services anytime and anywhere throughout the world, its pros and corns allow users to utilize globally.

Similarly its critical and serious privacy risks and issues are waiting for them as an interaction in liveliness and their access control. To advent these resources can now be accessed by almost each and everyone with mobile or any electronic devices. We observed some serious issues and lacking of privacy and security for user information's, services, environment, infrastructure, Data etc., plotted in Fig. 6. Researchers focused on many privacy issues and proposed as many preventive measures for the same. This paper proposes an approach for preventing user's privacy while accessing their chattels in PUc environment and helps the users to have a glance to know about PUc security issues and its privacy preserving seriousness in computing field in a matter of time.

A publicly audit cloud storage may reduce the cloud owners expertise and cloud users privacy threat. It also reduces the cost for data users and develops more trust on cloud providers. The trust on data storage may implicate by data coloring techniques. Trust overlay methods support for multiple data centers. The user's identity based crypto systems may reduce the misbehavior and certificates are unnecessary to prove the identity of a user, to protect the sensitive user information in mobile cloud a snoogle information retrieval search engine were developed. In healthcare systems the computer based assistance increased tremendously it requires efficient batter life for prolonged communication. A novel battery scheduling algorithm introduced evaluated with weighted round robin and greedy method.

Integrating sensors with healthcare system and monitoring are a challenging task. Patient's information dissemination may increase the risk factor in healthcare system. Pervasive environmental affective frameworks for healthcare system handle these issues and reduce the risk in patient monitoring. Public verifiability for remote data integrity checking and verification carried out without the concern of third party auditors. It may reduce the leakage of data to third party auditors. Collaborative context aware (CCA) information dissemination may lead to data integrity while communication of nodes in social networking systems. CCA and Markov process infers the data leakage in the publicly interlinked systems.

The EasiTia for traffic information acquisition system, for low signal noise ratio and a collaborative traffic information mechanism adopted as a pervasive traffic assistant for VANET. For ubiquitous environment a key agreement scheme with user authentication technique to minimize the leakage of secretes information form serves. The combination of lazy revocation, multi-tree structure and symmetric encryption is used to design an efficient privacy preserving framework for

the cloud storage. A security threat is introduced for key agreement scheme using elliptical curve discrete logarithm problem.

To preserve the vehicle user information privacy and anonymous authentication an efficient location based service (LBSs), double registration detection for users using Dynamic privacy preserving key management scheme (DIKE) are proposed with normal threshold technique. The way to improve the ubiquitous devices localization on human body to monitor healthcare system by mixed supervised and unsupervised time series analysis method. Rao et al., a plug-in for the internet browser integrated with double Authentication and Hybrid Obfuscation Technique to preserve the user data in cloud services. Moreover, by placing the key and data in different cloud environment by adopting the divide and rule policy.

Horizontally and vertically distributed datasets for privacy preserving clustering technique by adopting the Haar wavelet transforms (HWT) and scaling data perturbation (SDP) methodology to preserve the users information. A rapid prototyping was developed to improve the reliability of communication in a pervasive environment with a framework to improve the autonomous composition, failure detection, and recovery of services. In a typical end–end communication a stochastic analytical modeling framework using Holistic evaluation system was developed for mobility integrating.

5. Conclusion

In contemporary information technological era, the pervasive and ubiquitous computing emerges as next generation process of integration with human. The communication bespoke stratagems have facing new set of privacy preserving issue for an uninterrupted and a safe info transfer is highly recommended by global service providers. In this paper the proposed system focused on intelligent multi-agent model. It is a hybrid authentication technique to create end point secrecy preservation with a composite model using anomaly detection, hash based authentication and Diff–Hallman exchange protocol. It also acts as privacy preserving model for ensuring user's information's is well protected and to improve the demand of cloud storage by developing trust on service providers. This paper concentrates and arrives at a need and demand of coupled modular approach which framed as a policy to prevent and maintain the secrecy of cloud user, which is restricted as per the organizations agenda and limitations. Future research focuses to carry out and enhance the model with advance policy. A tool having its own privacy preserving framework which is partially interoperable with future cloud providers to compete the parley with the latest technologies emerges in the information technology industry.

Acknowledgments

This work is a part of the Research Projects sponsored under the Major Project Scheme, UGC, India, Reference No.: F.No.41-616/2012 (SR), dated 18 July 2012 and Department of Science & Technology (DST), INSPIRE fellowship, Government of India. The authors would like to express their thanks for their financial support offered by the Sponsored Agencies.

References

[1] Mitrovi Dejan, Ivanovi Mirjana, Budima Zoran, Vidakovi Milan. Radigost: interoperable web-based multi-agent platform. J Syst Soft 2014;90:167–78.

[2] Chandramohan D, Vengattaraman T, Dhavachelvan P. Data privacy breach prevention framework for the cloud service. John Wiley: Security Comm. Networks 2014:1–24. http://dx.doi.org/10.1002/sec.1054.

[3] Afzali Neda, Azmi Reza. MAIS-IDS: a distributed intrusion detection system using multi-agent AIS approach. Eng Appl Artif Intell 2014;35:286–98.

[4] Zambonelli Franco, Omicini Andrea, Anzengruber Bernhard. Developing pervasive multi-agent systems with nature-inspired coordination. Pervasive Mobile Comput 2014:1–17. http://dx.doi.org/10.1016/j.pmcj.2014.12.002.

[5] Murugaiyan SR, Chandramohan D, Vengattaraman T, Dhavachelvan P. A generic privacy breach preventing methodology for cloud service. Int J Grid High Perform Comput-IGI Global 2014;6(3):56–88. http://dx.doi.org/10.4018/ijghpc.2014070104.

[6] Pieters W et al. Effectiveness of qualitative and quantitative security obligations. J Inform Secur Appl 2014:1–14. http://dx.doi.org/10.1016/j.jisa.2014.07.003.

[7] Chandramohan D, Vengattaraman T, Dhavachelvan P, Baskaran R, Venkatachalapathy VSK. Fewss-framework to evaluate the service suitability and privacy in a distributed web service environment. Int J Model Simul Sci Comput 2014;5(1):1–37. http://dx.doi.org/10.1142/S1793962313500165.

[8] Abd-Eldayem. A proposed security technique based on watermarking and encryption for digital imaging and communications in medicine. Egypt Informat J 2013;14:1–13.

[9] Khedr. SRFID: a hash-based security scheme for low cost RFID systems. Egypt Informat J 2013;14:89–98.

[10] Chandramohan D, Vengattaraman T, Rajaguru D, Baskaran R Dhavachelvan P. A privacy preserving representation for web service communicators' in the cloud, vol. 115. In: 9th international conference on heterogeneous networking for quality, reliability, security and robustness, QSHINE-proceeding, Springer; 2013. p. 496–506. [ISBN: 978-1-936968-71-8].

[11] Soliman, Hikal, Nehal. A comparative performance evaluation of intrusion detection techniques for hierarchical wireless sensor networks. Egypt Informat J 2012;13:225–38.

[12] Chandramohan D, Vengattaraman T, Basha MSS, Dhavachelvan P. MSRCC–mitigation of security risks in cloud computing. Advances in intelligent systems and computing, vol. 176. Springer Book Series; 2012. p. 525–32.

[13] Tiwari Harshvardhan, Asawa Krishna. A secure and efficient cryptographic hash function based on NewFORK-256. Egypt Informat J 2012;13:199–208.

[14] Victer Paul P, Saravanan N, Jayakumar SKV, Dhavachelvan P, Baskaran R. QoS enhancements for global replication management in peer to peer networks. Future Gener Comput Syst 2012;28(3):573–82.

[15] Chandramohan D, Student Member, IEEE, Vengattaraman T, Dhavachelvan P. HPPC-hierarchical petri-net based privacy nominal model approach for cloud. In: IEEE-INDICON proceedings-0/12-2012; 2012. p. 1047–1052. [ISBN:978-1-4673-2272-0/12].

[16] Lin Jhih-Yi, Yen Yuo-Ju. Comments on a secret-key-privacy-preserving authentication and key agreement scheme. In: IEEE-genetic and evolutionary computing (ICGEC) 2011 fifth international conference; 2011. p. 168–171.

[17] Hao Zhuo, Zhong Sheng, Yu Nenghai. A privacy-preserving remote data integrity checking protocol with data dynamics and public verifiability. IEEE Trans Knowledge Data Eng 2011;23(9):1432–7.

[18] Wang Rui, Zhang Lei, Sun Rongli, Gong Jibing, Cui Li. EasiTia: a pervasive traffic information acquisition system based on wireless sensor networks. IEEE Trans Intell Transport Syst 2011;12(2):615–21.
[19] Anagnostopoulos Christos, Hadjiefthymiades Stathes, Zervas Evangelos. Information dissemination between mobile nodes for collaborative context awareness. IEEE Trans Mobile Comput 2011;10(12):1710–25.
[20] Venkatesan S, Dhavachelvan P, Chellapan C. Performance analysis of mobile agent failure recovery in e-service applications. Int J Comput Stand Interfaces 2010;32:38–43.
[21] Li Deyi. Trusted cloud computing with secure resources and data coloring. IEEE Trans Internet Comput 2010;14(5):4–22.
[22] Wang Cong, Ren Kui, Lou Wenjing, Li Jin. Toward publicly auditable secure cloud data storage services. IEEE Trans Network 2010;24(4):19–24.
[23] Zhang Chi, Zhang Yanchao, Fang Yuguang. An identity-based security system for user privacy in vehicular ad hoc networks. IEEE Trans Parallel Distrib Syst 2010;21(9):1227–39.
[24] Wang Haodong, Tan Chiu C, Li Qun. Snoogle: a search engine for pervasive environments. IEEE Trans Parallel Distrib Syst 2010;21(8):1188–202.
[25] Zheng Nenggan, Wu Zhaohui, Lin Man, Yang Laurence Tianruo. Enhancing battery efficiency for pervasive health-monitoring systems based on electronic textiles. IEEE Trans Inform Technol Biomed 2010;14(2):350–9.
[26] Taleb Tarik, Bottazzi Dario, Nasser Nidal. A novel middleware solution to improve ubiquitous healthcare systems aided by affective information. IEEE Trans Inform Technol Biomed 2010;14(2):335–49.
[27] Vengattaraman T, Abiramy S, Dhavachelvan P, Baskaran R. An application perspective evaluation of multi-agent system in versatile environments. Int J Expert Syst Appl 2011;38(3):1405–16.
[28] Abirami S, Baskaran R, Dhavachelvan P. A survey of Keyword spotting techniques for printed document images. Artif Intell Rev 2011;35(2):119–36 (2010).
[29] Huang RuWei, Yu Si, Zhuang Wei, Gui XiaoLin. Design of privacy-preserving cloud storage framework. In: IEEE-proceedings of the ninth international conference on grid and cloud computing; 2010. p. 128–132.
[30] Vengattaraman T., Dhavachelvan P. An agent-based personalized e-learning environment: effort prediction perspective. In: IEEE international conference on intelligent agent & multi-agent systems, IAMA 2009; 2009. p. 1–6. [ISBN: 978 1-4 244-4710-7].
[31] Lin Xiaodong, Liang Xiaohui, Shen Xuemin. A dynamic privacy-preserving key management scheme for location-based services in VANETs. IEEE Trans Intell Transport Syst 2012;13(1):127–39.
[32] Amini Navid, Sarrafzadeh Majid, Vahdatpour Alireza, Xu Wenyao. Accelerometer-based on-body sensor localization for health and medical monitoring applications. Pervasive Mobile Comput 2011;7:746–60.
[33] Chandramohan D, Vengattaraman T, Rajaguru D, Baskaran R, Dhavachelvan P. EMPPC-an evolutionary model based privacy preserving technique for cloud digital data storage service. IEEE-IACC Proc. 2013:89–95 [ISBN: 978-1-4673-4528-6].
[34] Rao TS, Venkat SP. A threat free architecture for privacy assurance in cloud computing. In: IEEE conference on services; 2011. p. 564–568.
[35] Hajian Sara, Azgomi Mohammad Abdollahi. A privacy preserving clustering technique for horizontally and vertically distributed datasets. ACM-Intell Data Anal 2011;15(4):503–32.
[36] Liao Chun-Feng, Jong Ya-Wen, Fu Li-Chen. Toward reliable service management in message-oriented pervasive systems. IEEE Trans Services Comput 2011;4(3):183–95.
[37] Chandramohan D, Vengattaraman T, Rajaguru D, Baskaran R, Dhavachelvan P. Hybrid authentication technique to preserve user privacy and protection as an end point lock for the cloud service digital information. In: IEEE-ICGHPC conference proceedings; 2011, p 1–4. [ISBN:978-1-4673-2594-3/13/$31.00].
[38] Bondavalli Andrea, Hamouda Ossama, Kaa niche Mohamed, Lollini Paolo, Majzik Istvan, Schwefel Hans-Peter. The HIDENETS holistic approach for the analysis of large critical mobile systems. IEEE Trans Mobile Comput 2011;10(6):783–96.
[39] Weiser Mark. Some computer science problems in ubiquitous computing. Commun ACM 1993;36(7):137–43.
[40] Abosamra, Hashem, Darwish. Securing DSR with mobile agents in wireless ad hoc networks. Egypt Inform J 2011;12:29–36.
[41] Li Wuquan, Zhang Ji-Feng. Distributed practical output tracking of high-order stochastic multi-agent systems with inherent non-linear drift and diffusion terms. Automatica 2014;50(12):3231–8.