Hidden Markov Model based Framework for User's Uniqueness in Pervasive Computing

Shivnandan Mandre
IT department
Samrat Ashok Technological Institute
Vidisha, India

Anil Suryavanshi
Asst. prof. IT department
Samrat Ashok Technological Institute
Vidisha, India

ABSTRACT
Pervasive computing technology endeavors to make simpler day-to-day life by providing mobile users with the means to make available out individual and business services by means of convenient and embedded devices. These technologies assure to increase yield through faultless communications and allow anytime, anywhere access to applications and services and the structures of smart homes and surroundings. Here in this paper Hidden Markov Model based Generation of User's Identity is proposed in Pervasive computing which provides efficient security from various attacks in Pervasive Computing and also provides efficient computational time and computational overhead.

Keywords
Pervasive Computing, Hidden Markov Model, Hash Function, User's Identity

1. INTRODUCTION
Visions of future computing backgrounds engage integrating small microelectronic processors and sensors into everyday things with the purpose of create them "smart." Smart things can discover their surroundings converse with other smart things and cooperate with human beings consequently selection customers to manage with their jobs in novel sensitive techniques. On the other pointer, this digitization of everyday exists will not simply permit computers to enhanced "recognize" achievements and objectives but also agree to others to examine and investigate such electronic documentations potentially generating a broad examination network of extraordinary level. New technologies like Radio Frequency Identification (RFID) and development in smart computing machines understands the globe of entirely connected devices to make available the suitable substances and repairs on the soar. Convergence of unusual wireless technologies a consequence into wireless network of various mechanisms with self-configuring potential and is expressional as Internet of Things (IOT). The idea of IOT is to join everything with computing, communication and sensing capability to the Internet. IOT encloses various choices of devices from RFID tags, sensor nodes to the yet shoes. Thus, IOT allow nomadic group effort and communication between users and devices between devices themselves and machines to repairs. Due to fast technical progressions in the wireless messages data coming from uncountable requests and services meet on user devices, communication infrastructure and the Internet are essential measurement of today's networked user. In IOT, communication and data excess is exaggerated due to objects, services, smart devices and sensors. Due to rising commands and scientific progressions in the wireless communications idea of IOT is increasing quickly [1, 2]. The International Telecommunications Union (ITU) liberated a report in 2005. This report has sketch out their idea of how networking particularly the Internet will develop in the face of ever-increasing amounts of interconnected consumers and devices, entitled IOT.

2. THEORETICAL BACKGROUND
With the increasing improvement of pervasive computing knowledge that are moving towards a period where context data will be essential for access control. Conventional access control representations like Mandatory Access Control (MAC), Discretionary Access Control (DAC), and Role-Based Access Control (RBAC) do not effort well in these circumstances for numerous explanations. Initially, contrasting conventional applications, inescapable computing requests more often than not do not have distinct security boundary–the entities an application will cooperate with or the resources that will be right of entries may not be recognized in progress. Second, these applications are also active in nature the accessing entities may transform resources need security may be formed or modified and an entity's right to use to reserves may change during the route of the request which create the resources security during application implementation enormously demanding. Third, universal computing requests employ the information of immediate objective spaces to give services; safety measures policies planned for such applications must consequently employ contextual information. Consequently, new access control representations and technologies are required for pervasive computing applications. Another method uses a certification authority. Some engagement the use of a proxy waitperson in order to give users admission to protected proxy identifications when and where desirable, without necessitating them to unswervingly accomplish their long-lived identifications [3].

3. CONTEXT AND CONTEXT-AWARENESS
The word context-aware can be described for unusual application regions and for different reasons. There are numerous explanations of context-awareness in the literature [4]. According to Schilit and Theimer [5], "a scheme is context-aware if it can give circumstance appropriate data and repairs to consumers and applications from the set of context categories, for example location, identification of in close proximity people, objects and transforms to those things." Almost immediately after them, Schilit et al. [6] also defined a context-aware scheme can familiarize yourself itself to the context." subsequently, many group defined context-aware schemes in a related way. For example, according to Dey [7], "a system can be context-aware if it employs context to give appropriate data and/or services to the consumer where

relevancy depends on users' job." According to Ryan et al. [8], "a system is context-aware if it has the capability to distinguish and intellect, understand and react to characteristics of a user's local situation and to the computing devices themselves." Dey and Abowd [9] describe context as "any data that can be used to characterize the circumstances of an entity that is measured appropriate to the communication between a customer and an application". According to Krish [10] "context is an extremely prepared mixture of data i.e. physical and conceptual resources that go ahead of the easy information's of who or what is where and when to comprise the condition of digital resources, people ideas and psychological condition, job circumstances, social relations and the limited work background to name a small amount of ingredients".

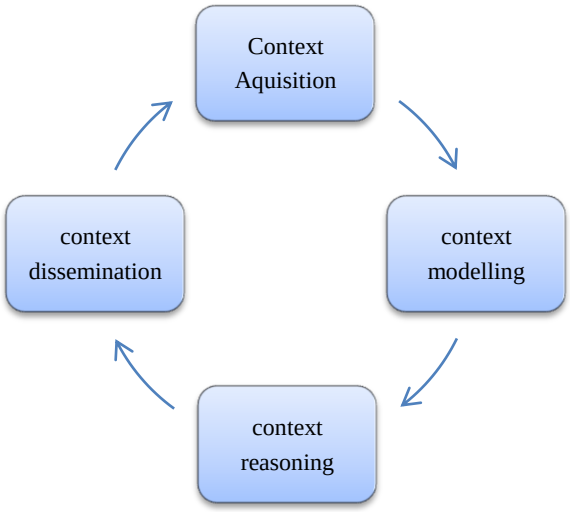

Figure1. Background life cycle

As portrayed in Figure 1, a context-aware organization shadows the life sequence process to bring contextual data. Gomez and Wrona [11] identified context data detection background data attainment and context information way of thoughtful as main ladders in a life sequence of context-aware organization. Bernardos et al. [12] recognized context acquisition, data processing, reasoning and decision as major phases in a characteristic context management system. After evaluation the life cycles of context-aware scheme, Perera et al. [13] consequential context acquisition, context reasoning, context modeling and context dissemination as four stages in a characteristic context management scheme.

- **Context data acquisition:** A context-aware system collects contextual data from the discovered context data providers and stores it in a context data warehouse for additional explanation. The context acquisition can also go behind pull and push modes. The pull mode permits context-aware system to demand contextual data, while in case of push mode, context data providers push context data to the context-aware scheme.
- **Context data modeling:** The contextual data is procedures in conditions of attributes, features, associations, quality-of context characteristics and the queries for synchronous context demands. Subsequently, the novel context data is organized and additional to the presented contextual data repository for use.
- **Context data reasoning:** A way of thinking methods makes easy applications to use the existing context data. With the purpose of set up a way of thoughtful method a single piece of context data or a collection of such data can be used.
- **Context data dissemination:** The applications need contextual data use context dissemination to obtain context. The context is disseminated using query and subscription techniques. In a query technique, the context management scheme can employ that query to generate results. In a subscription technique, the applications subscribe the conditions with a context management system that make available the results upon detecting an occurrence.

4. CONTEXT-AWARE SECURITY

Many offered computer networks observe with permit and reject based access control rule permit means granting right of entry when the consumer or device documentation matches with pre-stored documentations and reject means jamming access when the consumer or device documentation do not match with pre-stored credentials. This kind of scheme can be measured stationary in environment because it does not get into thought other issues for example, contextual data from the user or device situation while making permit and deny choices. But the IOT has a self-motivated situation, where elastic safety measures policies using contextual data can potentially enhance the efficiency of safety measures choices.

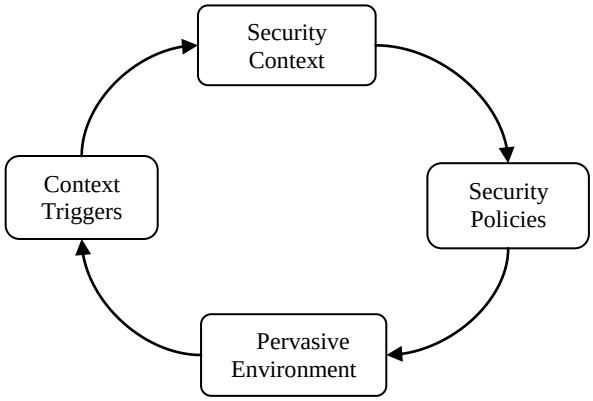

Figure2. Context-aware security

The security circumstance is characterized by Kouadri and Brézillon [14] as: "a set of data composed from the user's atmosphere and the application area and that is appropriate to the safety measures communications of both the customer and the application." Brézillon and Mostéfaoui [15] classify the safety measures context as circumstances where a security explanation thinks a set of data while making a definite security choice. Such as, while distinguishing an intrusion during statement security method may familiarize you to strong authentication technique. As depicted in Figure 2, originally the pervasive calculating situation is controlled by some security policy depending upon the initial context at that time [15]. Context triggers refer the dynamic changes in the environment with the passage of time. Security context refers this new context that is to be believed while organizing new security accomplishments as a consequence of the transform. A security policy specifies the rules and regulations that rule who has the access and who doesn't in each kind of situation. Thus, the security rule should be elastic sufficient to provide somewhere to stay changing contexts.

Strang and Linnhoff-popien [16] surveyed the applicable methods to demonstrating circumstance. The authors reviewed various methods to classified comparative to their core constituents and estimated regarding their correctness for

ever-present computing. Many context-aware requests based on different context forms have been expanded in past for a range of application domains. The presented methods to context information modeling are sorted into six categories [16] [17] [18], which are based on the data structures used for lying out and swapping background data in the individual system.

5. PERVASIVE COMPUTING

Pervasive Calculating [19] refers to the pattern and vision that data and communication technologies, digital services become frequently presented, personalized, and are even more effortlessly fixed into every day's life and work activities and procedures in various characteristics. With pervasive computing, the creation, replace storage and utilization of digital data potentially occur anytime and everyplace, while the computing devices and amenities per se are planned in an unremarkable way or become even indistinguishable to the consumers. It thus passes on to a post-desktop period of computing. In addition to the expression pervasive computing, we create repeated use of:

- Pervasive computing environment and pervasive system to refer to freely inter-connected computing amenities that be in the right place to a widespread logical and/or organizational range,
- Pervasive ICT and pervasive technologies in order to subsume the technological components and mechanisms that are here within such an atmosphere, and
- Pervasive applications are utilized to highlight that the objectives ideas focus on the application level.

As a consequence, employed technologies also have to fit with pre-existing conventions of day-to-day life and anticipations of potential consumers with the purpose of are unbeaten. Thus, the expansion of pervasive computing is frequently attended by technology assessment research [20]. This shall assure that technological expansion continues reliable with communal, ethical and legal views. Especially, inherent acceptance issues need to be identified before the real world deployment of pervasive applications.

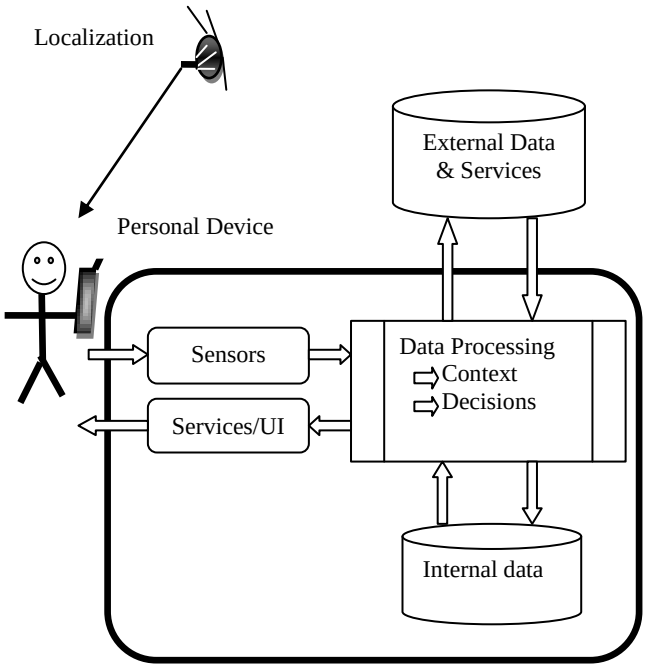

Figure3. Components of a Pervasive System

Analyzing a collaborative application scenario can highlight inherent conflicts with respect to underlying security and privacy requirements that are due to different personal, legal or organizational backgrounds of the participants [21]. Generally speaking, security requirements of parties and entities involved in digital transactions are often conflicting. In order to deal with this issue, the concept of multilateral security has be coined: multilaterally secure systems take into account security requirements of all involved parties and aim at balancing contrary interests in an acceptable way [22]. Consequently, after conflicting refuge necessities have been operated in contradiction of a multilaterally accepted compromise. Rather, the parties can concentrate on reaching a common goal.

6. LITERATURE SURVEY

In this paper author presents a new method [23] for authenticating user characteristics in universal situation using a non-intrusive behavior tracking method that presents smallest disruption to the user's activities. The method, known as Non-intrusive Identity Assertion System (NIAS), uses information of how the customer uses the environment's services to understand their distinctiveness. The method monitors customer behavior through recognizing certain kinds of action without the required for featured tracking of user behavior, thus minimizing intrusion on the user's standard activities. The method was estimated using a replicated area to evaluate its consistency. Experimental consequences show that the planned method can be applied in different circumstances such as exacting and undisturbed security settings by concerning various security policies. Here they also show that the method is mainly efficient where the situation has a combination of high and low security assets in which case consistency could exceed 99%.

In this paper author, gives a new technique important key delivery (QKD) make available information-theoretic security based on the laws of physics. Due to the deficiencies of real-life accomplishments on the other hand, there is a big gap between the theories and observe of QKD which has been newly developed by numerous important pony-trekking happenings. To fill this space, a new technique called measurement-device-independent QKD (mdiQKD), has been proposed [24]. It can eliminate all side-channels from the dimension unit, possibly the most susceptible part in QKD schemes thus present a clear opportunity in the direction of secure QKD realizations. Here, they can review the most recent expansions in the structure of mdiQKD, mutually with its suppositions, strengths and faults.

In this paper author [25] has to deliberate the confidentiality and safety suggestions of using pervasive computing to enlarge human memory. Here they explain a number of circumstances, summarize the explanation architectural construction chunks and recognize completely new kinds of security and privacy threats – specifically those connected to data security i.e. experience origin, data management i.e. establishing new models for digital memory possession, data integrity i.e. memory shrinking and recall encourage fail to remembering and witness privacy. Together these threats here compelling research confronts for the pervasive computing research community. Their involvements are three-fold:

- Here they emphasize universal memory expansion as a significant region of potential work for the community and provide a series of compelling application examples.
- We designate the fundamental architectural construction chunks of a forthcoming inescapable remembrance

development ecosystem.

- Based on construction they recognize a quantity of discretion and sanctuary pressures that provide research challenges for the community.

7. PROPOSED METHODOLOGY

The Hidden Markov Model (HMM) is an authoritative statistical means for network demonstrating reproductive arrangements that can be differentiated by an essential development producing a recognizable sequence of given model. HMMs have originate submission in several areas concentration in signal processing area and in scrupulous speech processing, but have also been functional with accomplishment to low level Natural Language Processing tasks such as part-of-speech attach a label to going on phrase break apart, and pull out objective information from manuscripts.

There is a big alteration amongst Markov Classical and Hidden Markov Classical. The Markov model contains a number of states in which transition probability is calculated from one government to additional forward and backward. But the model can't compute class value of the transition probability.

The figure shown below is the example set of Markov Model. The model contains two states Rain and Dry with their respective state transition probability as 0.4 and 0.6.

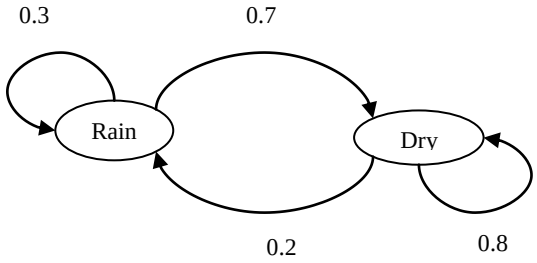

Figure4. Example of Markov Model

While Hidden Markov model computes state transition probability from one national to additional and also contains some hidden layers in between that is use store class value from the one state to another. The figure shown below is the state transition probability of HMM. It contains two hidden layers as low and high.

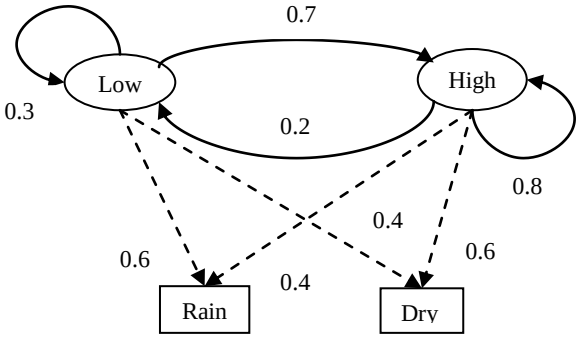

Figure5. Example of Hidden Markov Model

The Planned Procedure implanted here consists of following phases:

1. Create a Simulation Environment of Pervasive Computing with 'N' of Users.
2. Each of the Users contains a set of Identity or Node or State with Devices such as Smart cards or Tags.
3. Each of the Users in the group is attached with some other Node or User by some transition state.
4. Whenever user performs any activity probability is computed and attribute is attached to the respective User.
5. The Users identity is then verified and authorized and access is allowed for the user.

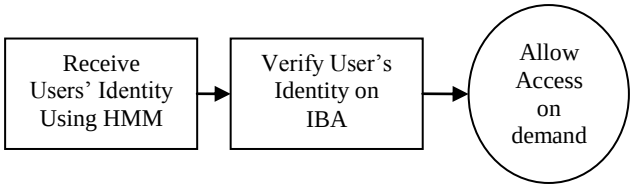

Figure6. Working of the Proposed Work

Flow Chart of Proposed Methodology

The Proposed Methodology implemented here uses Pervasive Computing Environment including Hidden Markov Model for the Verification of User's Identity of User. As Show in the figure below first of depending on the number of user's States are taken and each of the state is attached with some other State by some probability, so that if any user want to access data of other user probability is match and verified accordingly.

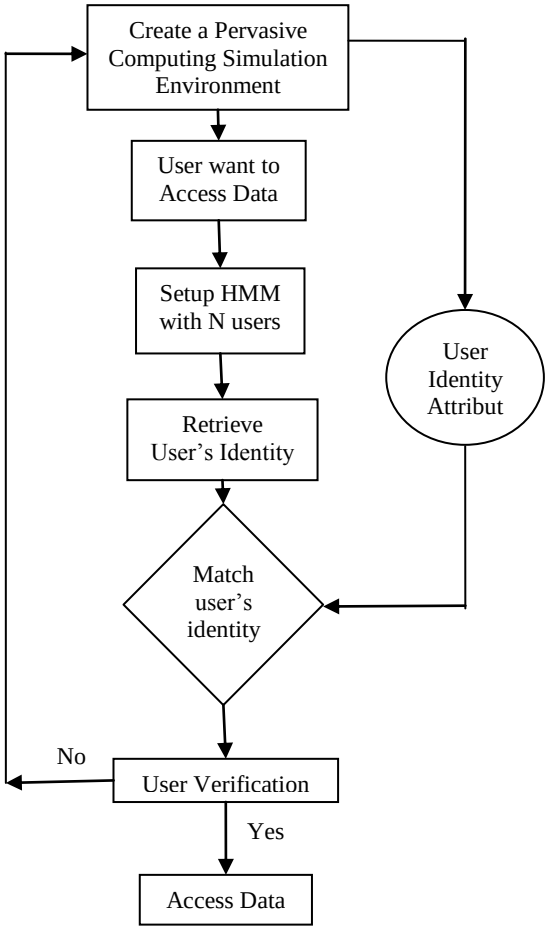

Figure7. Flow Chart of the Proposed Work

8. RESULT ANALYSIS

The Table shown below is the analysis and Assessment of the

Existing Non-Intrusive Technique and the proposed methodology. The Planned procedure implemented here provides high reliability User's Access in comparison.

Table1. Comparison of Reliability of the System

	Reliability %	
NL / NH	Existing Wok	Proposed Work
1	97.2	98.6
2	97.6	98.9
3	98	99.1
4	98.4	99.3
5	98.6	99.5
6	99	99.6
7	99.3	99.8

The Table shown below is the analysis and Assessment of the Existing Non-Intrusive Technique and the proposed methodology. The Planned procedure implemented here provides Global Assertion Value for User's Access in comparison.

Table2. Analysis of Global Assertion Value at $\Delta g = 1$

	Global Assertion Value at g=1	
Time	**Existing Work**	**Proposed Work**
7:00	0.4	0.47
8:00	0.5	0.53
9:00	0.6	0.67
10:00	0.7	0.74
11:00	0.8	0.86
12:00	0.9	0.93
13:00	1	1

The Figure shown below is the analysis and Assessment of the Existing Non-Intrusive Technique and the proposed methodology. The Planned procedure implemented here provides high reliability User's Access in comparison.

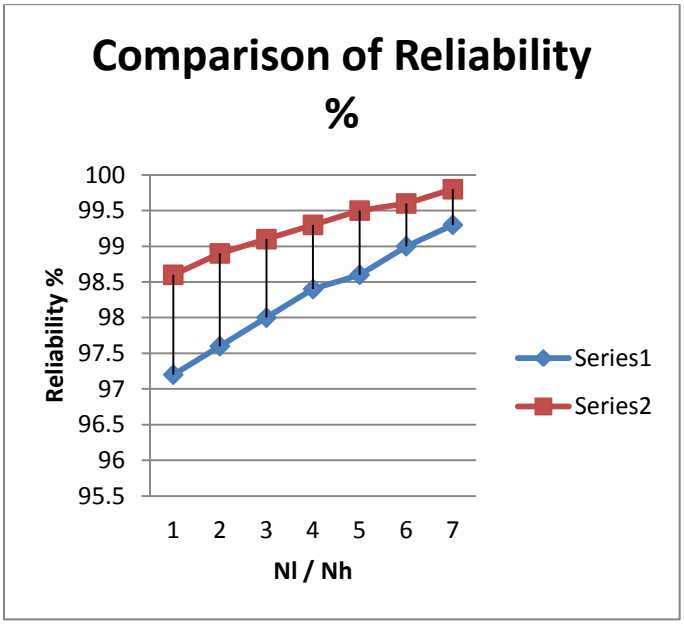

Figure8. Analysis & Comparison of Reliability

The Table shown below is the analysis and comparison of various security attacks possible using Hidden Markov Model based on Demand User's Identity Verification.

Table3. Analysis of Security from various attacks

S. No.	**Security Attacks**	**Existing Work**	**Proposed Work**
1	Password Impersonation	No	Yes
2	Password Guessing Attack	Yes	Yes
3	Confidentiality	No	Yes
4	Public Verifiability	Yes	Yes
5	DoS Attack	Yes	Yes
6	Insider Attack	No	Yes
7	Denning Sacco Attack	Yes	Yes
8	DDoS Attack	No	Yes
9	Outsider Attack	Yes	Yes
10	Online Dictionary Attack	Yes	Yes
11	Offline Dictionary Attack	Yes	Yes
12	Server Masquerade Attack	Yes	Yes
13	Integrity	Yes	Yes
14	Unforgeability	Yes	Yes
15	Non-Repudiation	Yes	Yes
16	Forward Secrecy	Yes	Yes
17	Additional Authentication	No	Yes

The Figure shown below is the analysis and Assessment of the Existing Non-Intrusive Technique and the proposed methodology. The Planned procedure implemented here provides Global Assertion Value for User's Access in comparison.

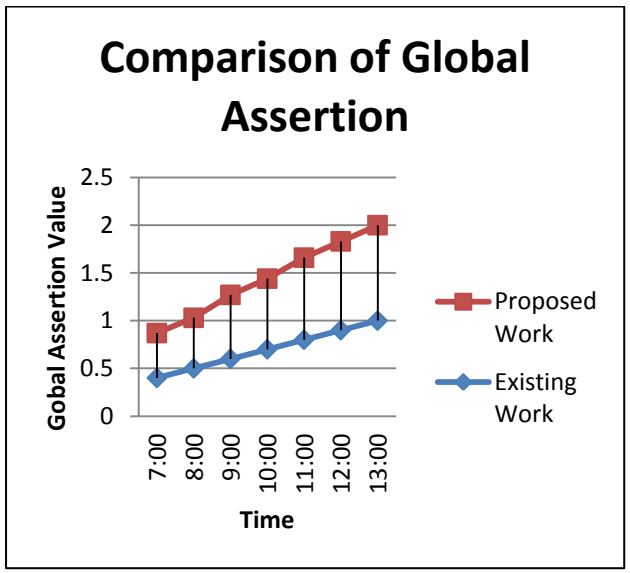

Figure9. Comparison of Global Assertion Value at $\Delta g = 1$

9. CONCLUSION

Although, developing authentication and access control mechanisms has been an active research areas among researchers, but mostly the existing mechanisms work on the principles of user credential based approach. While a profound theoretical and technical knowledge is required to devise security mechanisms, additional care has to be taken in order to support a practical use. While explicit user interfaces tend to disappear within pervasive system, many additional interfaces to the real world emerge. The proposed Methodology implemented here for the generation of user's Identity using Hidden Markov Model for the Efficient Revocation of User's and efficient Computational Time and Overhead.

Although the methodology implemented for the verification of user's Identity using Hidden Markov Model is efficient but further implemented can be done for various other environments such as grid computing and cloud computing.

10. REFERENCES

[1] J. P. Conti, "The Internet of Things," In Proceedings of IEEE Communication Engineering, Volume: 4, pp: 20-25, December – January 2006.

[2] Qian Xiaocong, and Zhang Jidong, "Study on the Structure of "Internet of Things (IOT)" Business Operation Support Platform," In Proceedings of 12th IEEE International Conference on Communication Technology (ICCT), pp: 1068-1071. Nanjing-China, November 11-14 2010.

[3] Barton T, Basney J, Freeman T, Scavo T, Siebenlist F, Welch V, et al. Identity federation and attribute-based authorization through the globus toolkit, shibboleth, gridshib, and myproxy. In: Proc of 5th annual PKI R&D workshop, April 2006.

[4] S. Poslad, "Ubiquitous Computing: Smart Devices, Environments and Interactions," Wiley Publishing, 2009.

[5] B. Schilit and M. Theimer, "Disseminating active map information to mobile hosts," IEEE Networks, 8(5):, pp. 22-32, 1994.

[6] B. Schilit, N. Adams, and R. Want, "Context aware computing applications," In Proceeding of 1st International Workshop on Mobile Computing Systems and Applications, 1995, pp. 85-90.

[7] A. K. Dey, "Providing Architectural Support for Building Context Aware Applications," PhD thesis, Computer Science, Georgia Institute of Technology, Atlanta, November, 2000.

[8] N. Ryan J. Pascoe, and D. Morse, "Enhanced reality fieldwork: the context aware archaeological assistant," In V. Gaffney, M. van Leusen, and S. Exxon (eds) Computer Applications in Archaeology, British Archaeological Reports, 1997.

[9] A. K. Dey and G. D. Abowd, "Towards a better understanding of context and context awareness," In Proceedings of the (HUC '99), 1999, pp. 304-307.

[10] D. Kirsh, "The Context of Work, Human-Computer Interaction," vol. 16, 2001, pp. 305-322.

[11] K. Wrona and L. Gomez, "Context-aware security and secure context-awareness in ubiquitous computing environments," Autumn Meeting of Polish Information Processing Society, 2004, pp.255-265.

[12] A. Bernardos, P. Tarrio, and J. Casar, "A data fusion framework for context-aware mobile services," IEEE International Conference on Multisensor Fusion and Integration for Intelligent Systems, 2008, pp. 606 –613.

[13] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, "Context aware computing for the internet of things: A survey," IEEE, 16, 2014, pp. 414-454.

[14] G. K. Mostéfaoui and P. Brézillon, "Modeling Context-Based Security Policies with Contextual Graphs," In Proceedings of (PERCOMW '04). IEEE Computer Society, 2004, pp. 28-32.

[15] P. Brezillon and G. K. Mostefaoui, "Context-based security policies: a new modelling approach," Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops, March 2004, pp.154,158.

[16] T. Strang and C. Linnhoff-Popien, "A Context Modelling Survey," In Workshop on Advanced Context Modelling, Reasoning and Management, UbiComp 2004, pp. 1-8.

[17] S. Vuppala et al., "uBiquitous, secUre inTernet-of-things with Location and contEx-awaReness," BUTLER project, D2.1 -Requirements, Specifications and Security Technologies for IoT Context-Aware Networks, October 2012, pp. 1-171.

[18] C. Bettini et al., "A survey of context modelling and reasoning techniques," Pervasive Mob. Comput. 6, (2), April 2010, pp. 161-180,.

[19] M. Satyanarayanan. Pervasive Computing: Vision and Challenges. IEEE Personal Communications, 8(4):10 – 17, 2001.

[20] J. Heesen and O. Siemoneit. Opportunities for Privacy

and Trust in the Development of Ubiquitous Computing. International Review of Information Ethics (IRIE), 8:47–52, 2007.

[21] S. F. Gürses and T. Santen. Contextualizing Security Goals: A Method for Multilateral Security Requirements Elicitation. In Sicherheit ’06, pages 42–53, 2006.

[22] K. Rannenberg. Multilateral Security - a Concept and Examples for Balanced Security. In Workshop on New Security Paradigms (NSPW ’00), pages 151–162. ACM Press, 2000.

[23] Al-Karkhi A et al. Discreet verification of user identity in pervasive computing environments using a non-intrusive technique. Comput Electr Eng (2014).

[24] Qinghua Shen, Xiaohui Liang, Xuemin (Sherman) Shen, Xiaodong Lin, “Exploiting Geo-Distributed Clouds for a E-Health Monitoring System With Minimum Service Delay and Privacy Preservation” IEEE Journal Of Biomedical And Health Informatics, Vol. 18, No. 2, March 2014.

[25] Nigel Davies, Adrian Friday, “Security and Privacy Implications of Pervasive Memory Augmentation” IEEE, 2015