*International Journal of Current Research and Modern Education (IJCRME)*
*Impact Factor: 6.725, ISSN (Online): 2455 - 5428*
*(www.rdmodernresearch.com) Volume 2, Issue 1, 2017*

# A HOME BASED SECURITY MECHANISM USING PAIRED KEY FOR SENSOR TO CLOUD COMMUNICATION

**Diljeet Singh Makkar* & C. Harisharan Aggarwal****
* M.Tech Student, Department of ECE, Guru Gobind Singh College of Engineering and Technology, Guru Kashi University, Talwandi, Bathinda, Punjab
** Head, Department of ECE, Guru Gobind Singh College of Engineering and Technology, Guru Kashi University, Talwandi, Bathinda, Punjab

**Cite This Article:** Diljeet Singh Makkar & C. Harisharan Aggarwal, "A Home Based Security Mechanism Using Paired Key for Sensor to Cloud Communication", International Journal of Current Research and Modern Education, Volume 2, Issue 1, Page Number 184-192, 2017.



**Abstract:**

IoT-related health care system are based on the vital description of the IoT as a network of devices that connect directly with each other to capture and share important data through a secure service layer as SSL that connects to a central command and control server in the cloud. The major objective of the proposed model is to increase the level of the security and based security model for the secure information propagation among the house panel and the cloud based monitoring system. In this project, an urgent need for research in user data privacy in the cloud is established and the risks of not achieving it are outlined. Proposed scheme is preventive rather than detective approach. Preventive approach in the proposed model is based on key exchange model for the user data privacy, integrity and data confidentiality. Also the proposed method is capable to protect against the security breach attacks on the IoT databases. The results have proved the effectiveness of the proposed solution. Hence the overall security implementation has imposed over the complete communication taking place between the house panels, remote panels and the cloud based house security monitoring under the proposed model. The proposed model is based upon the authentication.

**Key Words:** IoT, GPS, AES & SNR

## 1. Introduction:

There is no shortage of prediction that how the Internet of Things i.e. IoT is going to developed in healthcare by dramatically at lowering cost and improving quality. Internet of Things (IoT)-driven systems are making it possible to totally reduce costs and improving health by increasing the availability and quality of care. These include sensors that to collect patient data, microcontrollers are process, analyze band wirelessly communicate the data, microprocessors that allow rich graphical user interfaces, healthcare specific gateway through which sensor data is further analyses and sent to the cloud. As the First Thing First to Understanding the IoT that the IoT-related health care system are based on the vital description of the IoT as a network of devices that connect directly with each other to capture and share important data through a secure service layer as SSL that connects to a central command and control server in the cloud.

The emergence of the IoT, in which devices connect directly to data and to each other, is important for two reasons. First is as in advance sensor and connectivity technology are allowing devices to collect the data, record and analyze. In the healthcare, this means able to collect patient data over time that can be used to help enable preventive care, allow prompt diagnosis of sensitive complications and promote understanding of how a therapy is helping improve a patient's parameters [1, 3]. Second is the ability of devices to collect data on their own and removes the limitations of human-entered data by automatically obtaining the data doctor's need; at the time and in the way they need it. The automation reduces the risk of error and as fewer errors can mean increased efficiency, lower costs and improvements in quality in just about any industry. But it is of particular interest in healthcare, where human error can literally be the difference between life and death [3]. IoT concepts have already been adopted in many areas such as energy as examples of smart lighting, smart grig and industrial automation [4]. In the clinical care as Hospitalized Patients whose physiological status requires close attention can be constantly monitored using IoT-driven, non-invasive monitoring. Thos type of solution employs sensors to collect complete physiological information and uses gateways and the cloud to analyze and store the information and then send the analyzes data wirelessly to caregivers for further analysis and review [6]. In the remote monitoring, there are many people all over the world whose health may suffer because they do not have ready access to useful health monitoring. But small and powerful wireless solutions connected through the IoT are now making it possible for monitoring to come patient health data from a variety of sensors, apply complex algorithms to analyze the data or information and then share it through wireless connectivity with medical professionals who can make appropriate health recommendations [5, 6].

### Smart Cities and IoT Integration:

Smart town is that the product of accelerated development of the new generation information technology and knowledge-based economy, supported the network combination of the net, telecommunications

network, broadcast network, wireless broadband network and different sensors networks wherever Internet of Things technology (IoT) as its core. The most options of a wise town embody a high degree of knowledge technology integration and a comprehensive application of knowledge resources. The essential parts of urban development for sensible town ought to embody smart technology, good trade, good services, good management and good life. The Internet of Things is concerning putting in sensors (GPS, optical device scanners, etc.) for everything, and connecting them to the net through specific protocols for info exchange and communications, so as to realize intelligent recognition, location, tracking, observation and management. With the technical support from IoT, good town got to have 3 options of being instrumented, interconnected and intelligent. Solely then a wise town are often shaped by group action of these intelligent options at its advanced stage of IOT development. The explosive growth of good town and net of Things applications creates several scientific and engineering challenges that decision for ingenious analysis efforts from each world and trade, particularly for the event of economical, scalable, and reliable good town supported IoT.

**2. Related Work:**

Rosenthel et al. [11] had taken efforts to provide advantage of cloud computing for biomedical informatics (BMI) community for sharing medical data and applications. Rolim et al. [10] proposed a system for automating the task of collecting patient's crucial health data through sensor network attached to legally authorized medical devices and storing this data to medical centre's "cloud" for handling, executing, and sharing. Jacob et al. [9] worked upon development of remote patient monitoring (RPM) system supporting universal serial bus plug-in. Pandey et al. [34] developed a prototype system for analysing ECG signal by collecting electrocardiogram (ECG) data in real-time from patients. Ahnn et al. [1] proposed a distributed, energy efficient electronic health platform called mHealthMon in which distributed P2P network was created among mobile patients to access patient data collected by sensor from cloud computing-based storage. Wan et al. [4] conducted a study on high packet drop and poor network performance because of environmental obstacles. Almashaqbeh et al. [3] proposed real-time remote health tracking system for non-hospitalized patients. This system divided the cloud architecture as local one that contains patients and hospital medical staff, and a global cloud that contains the outer world. Wang et al. [2] discussed that in traditional IT solutions, the IT services were hosted under complete physical and personnel controls whereas, cloud computing shifted the application and databases phase to large data centre servers on the Internet. Doukas et al. [1] discussed about the application of Cloud Computing in healthcare services to update and retrieve patient health information. Fan et al. [6] proposed a "Data Capture and Auto Identification Reference" (DACAR) platform for developing eHealth applications equipped with authentication, integrity, confidentiality, authorisation, secure data transmission.

**Algorithm:**

The proposed algorithm is for the user data privacy in the Internet of Things for various applications system will be a combination of data compression, encryption and authentication schemes. The new hybrid user privacy model will ensure that the security level hardening for the secure data transfers in the IoT systems. The confidentiality of the user sending the data will be achieved by using the secure key exchange between the Internet of Things IoT devices and online controllers and storage databases. The secure key exchange model will be update in the proposed model than the existing user privacy solution. The key table sharing will be performed in the neighbor building state of the security model. To take on the data integrity, the encryption algorithm will be used. The encryption algorithm will ensure the privacy of the user data by making the data unreadable during data transmissions between the medical databases and IoT sensors. Also data encryption and compression schemes would be applied to the IoT data security mechanism to protect the user data privacy. The user data privacy will be increase to a level higher by using the data encryption using encryption algorithm better than AES, which must be capable of protecting the user data privacy more effectively than the normal data transmission. The data compression will be added to the security mechanism to reduce the data size of the authentication data which will be increased using the encryption mechanism.

**3. Results:**

**Time Based Analysis:**

The time taken for various procedures in the key exchange scheme has been recorded during the sensor communication in the proposed architecture simulation in the MATLAB simulator. The elapsed time has been recorded for various procedures: Time for Key generation, Time for key sharing or transfers, Time for key verification. The graph represents the key transfer time and key verification time recorded during the various key exchange intervals in the simulation. The key exchange interval has been set to 1 second in the simulation. It means the key is being exchanged every second between the two ends of the communication link in the sensor node network. The Average time has been taken for key transfer time at 2.01 seconds and 2.02 seconds for the key verification time. The proposed model has taken the maximum of 2.04 seconds for the key verification where the lowest value remains at the 2.01 seconds, whereas the key verification time has been recorded lowest at 2.07 seconds and highest at 2.15 seconds.

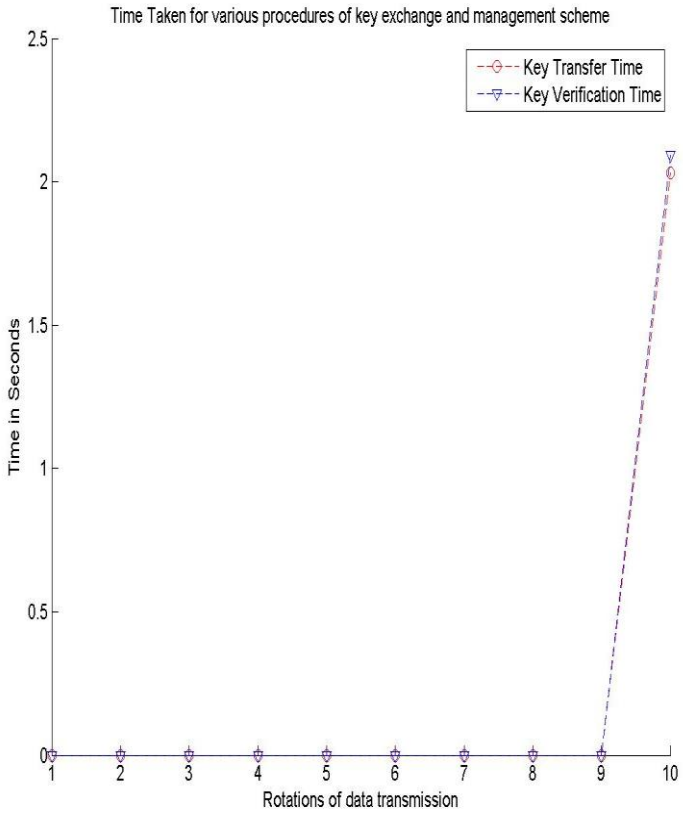


Figure a: Line Graph presentation of key transfer and verification schemes

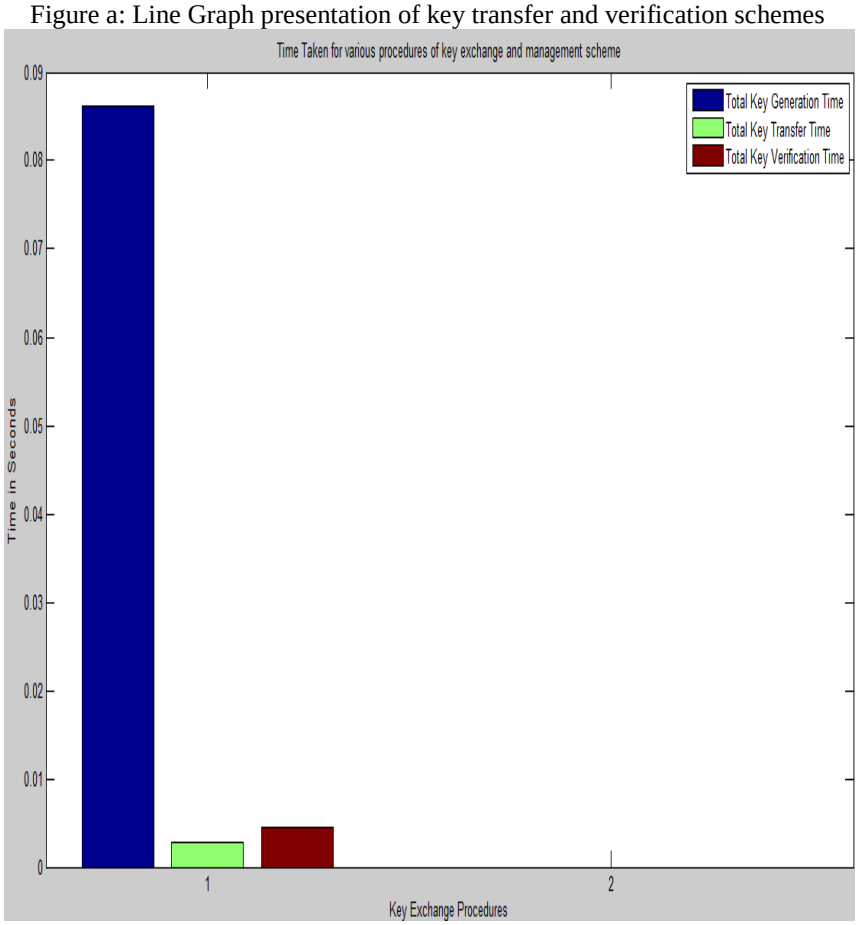


Figure b: Bar Graph presentation of key generation, key transfer and verification schemes

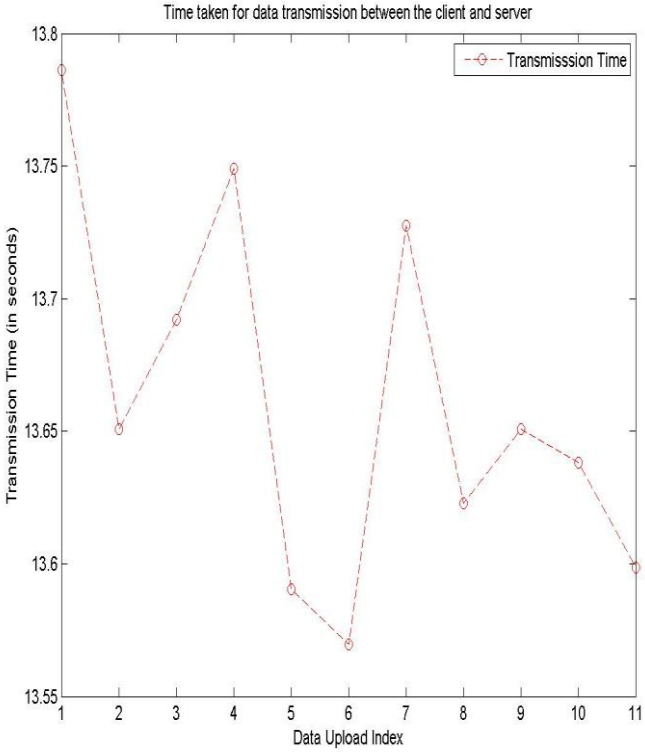


Figure c: Time taken for data transmission between the client and server

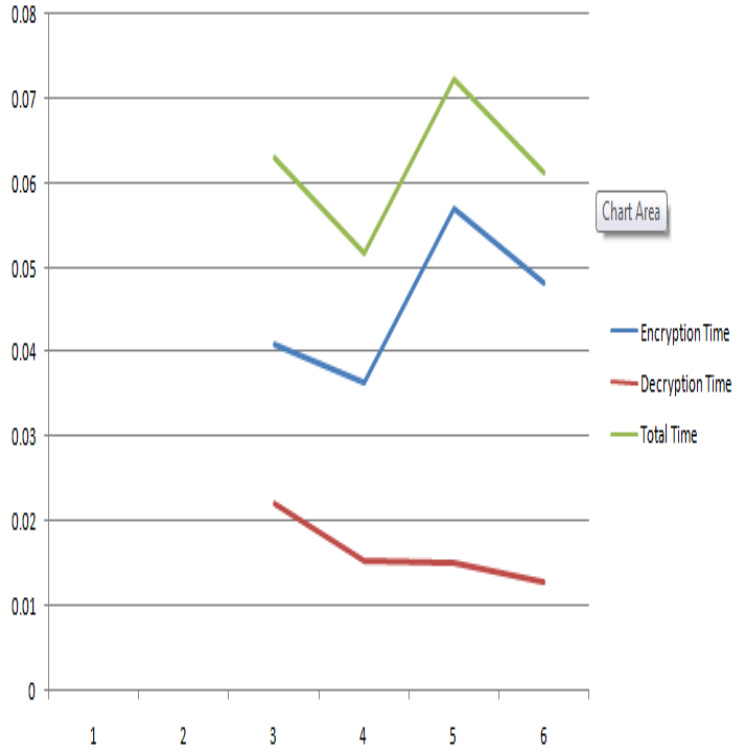


Figure d: The elapsed time graph for encryption and decryption process

**Entropy Analysis:**

Entropy is the quantitative measure of disorder or randomness in a system. High entropy means higher security. Entropy is calculated for every individual bit in the key table. The entropy of an individual key is given by the sum of the key bits over the entropy of individual bits.

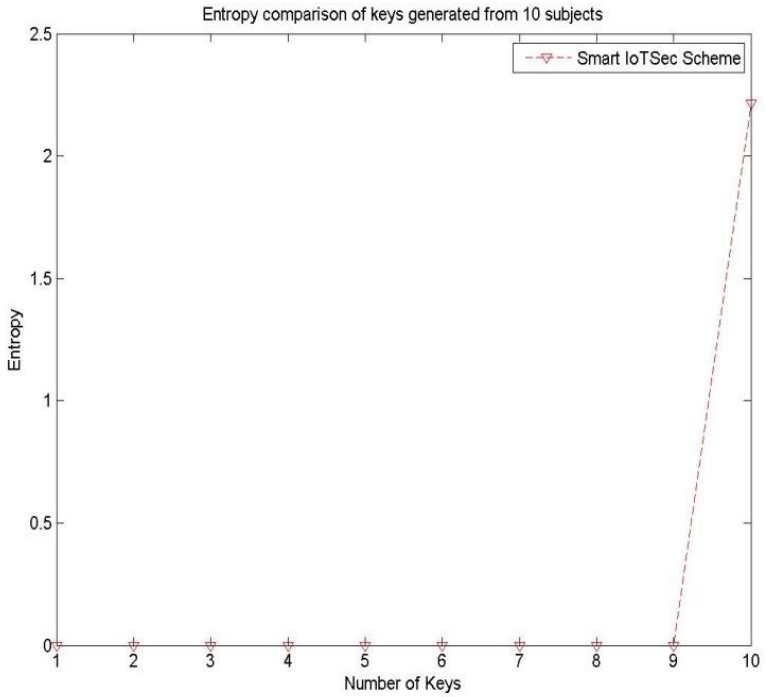


Figure e: Entropy comparison of keys generated for testing subjects

**Probability Analysis:**

The performance of the proposed model for the level of security has been evaluated using the parameters of key connectivity at deployment and the probability of key exposure of the keys being exchanged between the two ends.

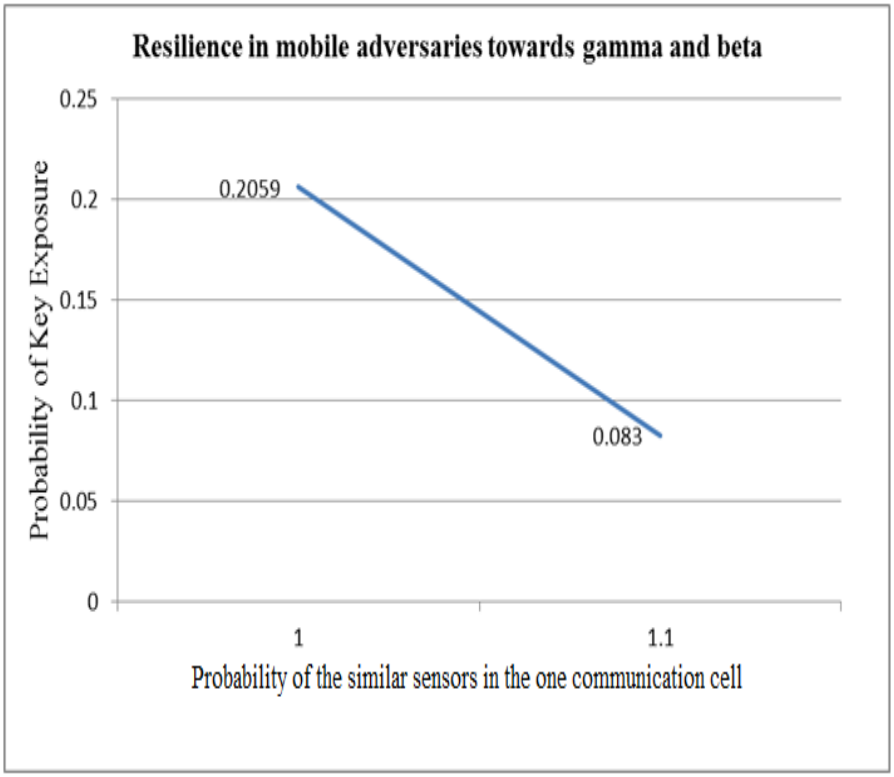


Figure f: Calculation of key exposure probability.

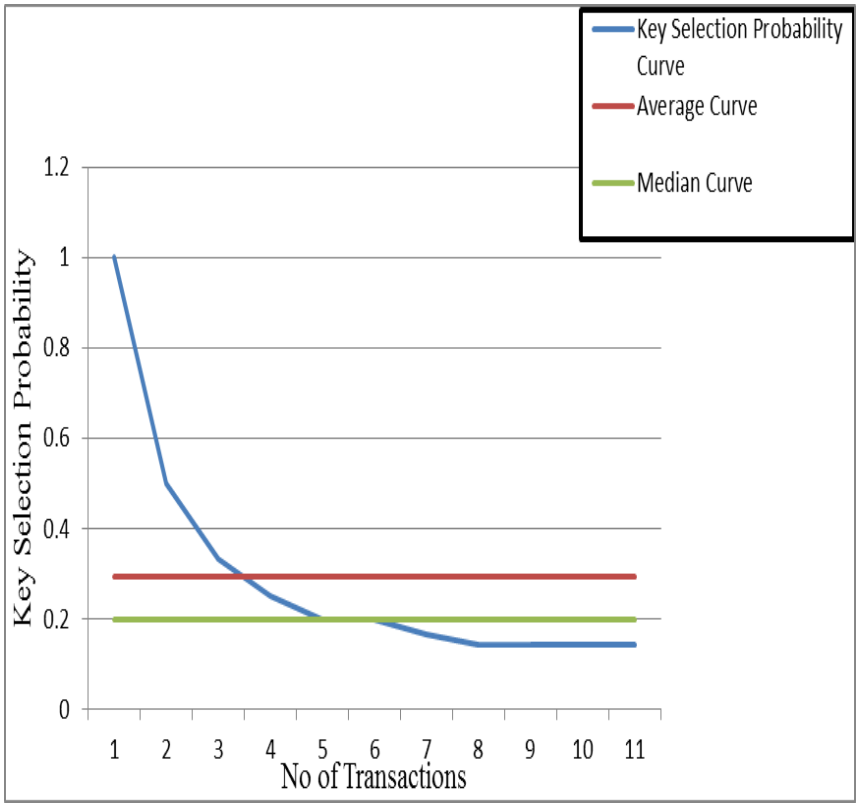


Figure g: Calculation of Key selection probability

**Memory Consumption Analysis:**

The memory consumption indicates the memory overhead by the proposed key management. The memory consumption is calculated by measuring the difference between memory usage recorded before and after the key management process.

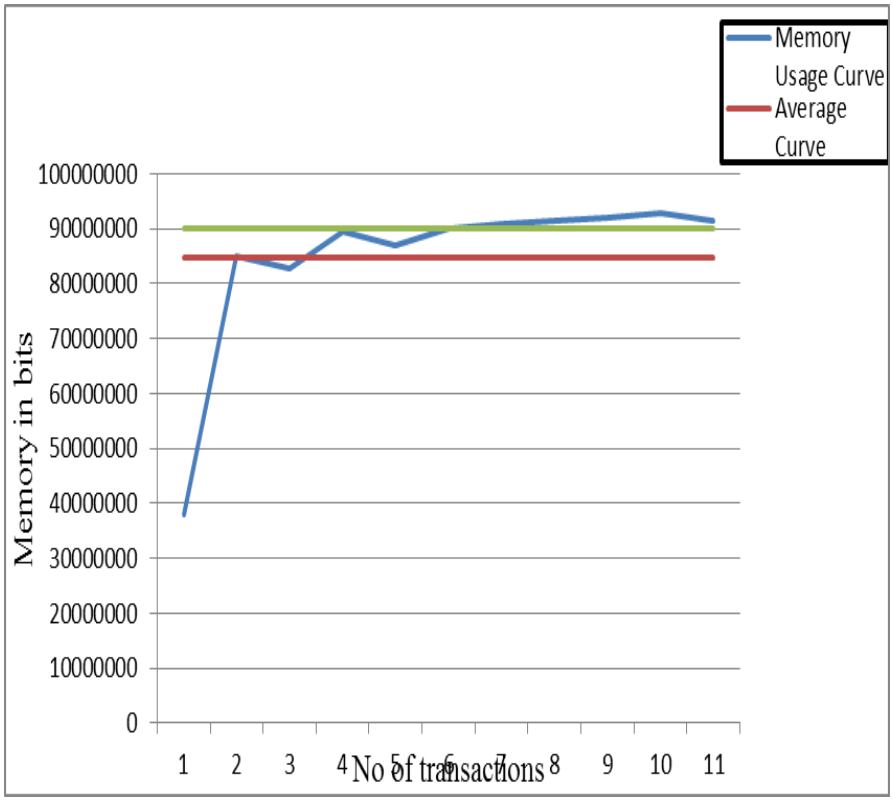


Figure h: Memory consumption by the key management process on the IoT node

**Time Based Comparison:**

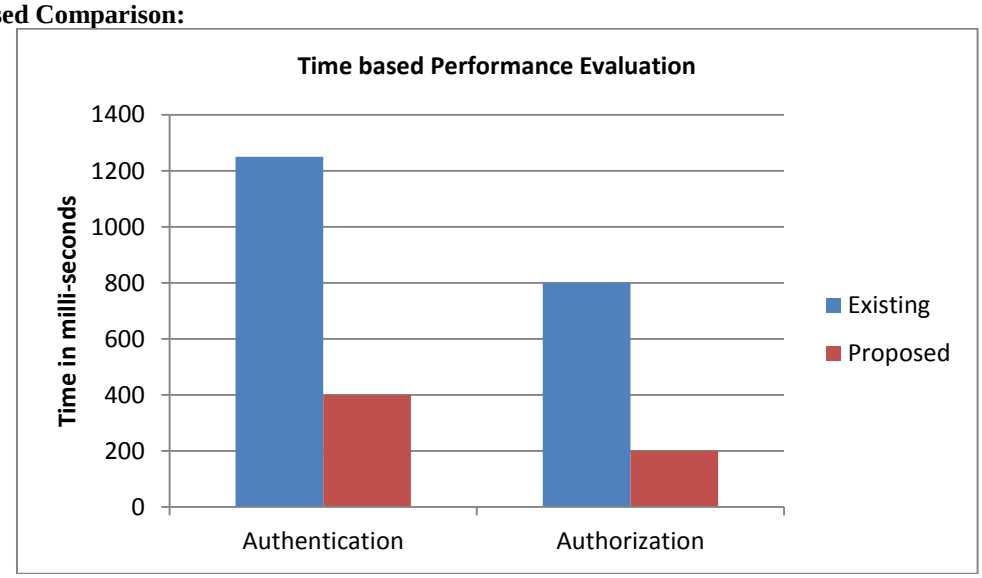


Figure i: Time based comparative analysis of the proposed model against existing model

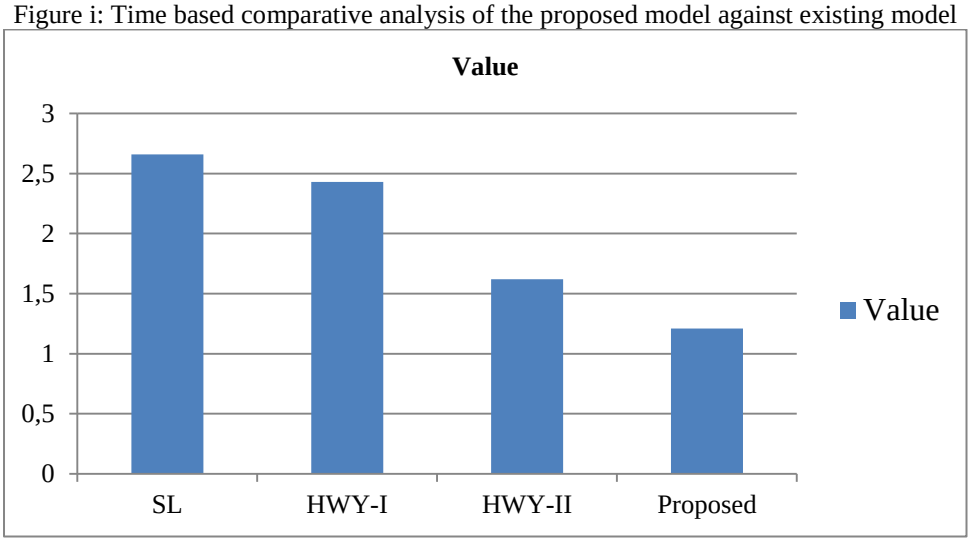


Figure j: Time based comparative analysis of the proposed model against different models

**4. Conclusion:**

The recent advancements in remote IoT systems endorsed significant concerns from IT industry(Amazon, Microsoft, Google etc.) that provide ubiquitary and conveniently deployable IoT systems. IoT monitoring sensor networks' based on cloud (IoT-MSN) is collection of number of IoT nodes attached to centralized communication node and an entrance for each node connecting through wireless connections. In this project, an urgent need for research in user data privacy in the cloud is established and the risks of not achieving it are outlined. Proposed scheme is preventive rather than detective approach. Preventive approach in the proposed model is based on key exchange model for the user data privacy, integrity and data confidentiality. Also the proposed method is capable to protect against the security breach attacks on the IoT databases. The results have proved the effectiveness of the proposed solution.

**5. Future Work:**

In future, the proposed model can be enhanced to work more efficiently and quicker. The approach would be enhanced to protect against many types of attacks with one security solution. Also the elapsed time will be improved to increase the speed of the proposed approach. The proposed model approach can be compared with other efficient approaches available for the authentication of cloud based IoT management services.

**6. References:**

1. Kumar, Adarsh, Krishna Gopal, and Alok Aggarwal. "Simulation and analysis of authentication protocols for mobile Internet of Things (MIoT)." In Parallel, Distributed and Grid Computing (PDGC), 2014 International Conference on, pp. 423-428.IEEE, 2014.
2. Lee, Jun-Ya, Wei-Cheng Lin, and Yu-Hung Huang. "A lightweight authentication protocol for internet of things." In Next-Generation Electronics (ISNE), 2014 International Symposium on, pp. 1-2. IEEE, 2014.

3. Abomhara, Mohamed, and Geir M. Koien. "Security and privacy in the Internet of Things: Current status and open issues." In Privacy and Security in Mobile Systems (PRISMS), 2014 International Conference on, pp. 1-8. IEEE, 2014.
4. Ali, S. T., Sivaraman, V., & Ostry, D. (2014). Authentication of lossy data in body-sensor networks for cloud-based healthcare monitoring. Future Generation Computer Systems, 35, 80-90.
5. Khan, F. A., Ali, A., Abbas, H., & Haldar, N. A. H. (2014). A Cloud-based Healthcare Framework for Security and Patients' Data Privacy Using Wireless Body Area Networks. Procedia Computer Science, 34, 511-517
6. Peng, X., Zhang, H., & Liu, J. (2014). An ECG Compressed Sensing Method of Low Power Body Area Network. TELKOMNIKA Indonesian Journal of Electrical Engineering, 12(1), 292-303.
7. Hernandez-Ramos, Jose L., Marcin Piotr Pawlowski, Antonio J. Jara, Antonio F. Skarmeta, and Latif Ladid. "Toward a Lightweight Authentication and Authorization Framework for Smart Objects". Selected Areas in Communications, IEEE Journal on 33, no. 4 (2015): 690-702.
8. Anu Bala, Munish Bansal, Jagpreet Singh, "Performance Analysis of MANET under Blackhole Attack", ICNC, vol. 1, pp. 141-145, IEEE 2009.
9. Anuj K. Gupta, Dr. Harsh Sadawarti, "Performance analysis of AODV, DSR & TORA Routing Protocols", IACSIT, vol. 2, no. 2, vol. 226-231, IJET, 2010.
10. Asma Tuteja et. al, "Comparative Performance Analysis of DSDV, AODV and DSR Routing Protocols in MANET using NS2", ICACE, pp. 330-333, IEEE 2010.
11. Chia-Chen Hung, Hope Chan, and Eric Hsiao-Kuang Wu "Mobility Pattern Aware Routing for Heterogeneous Vehicular Networks" (IEEE WCNC 2008).
12. Fuad A. Ghaleb, M. A. Razzaque, Ismail FauziIsnin "Security and Privacy Enhancement in VANETs using Mobility Pattern" (IEEE, 2013).
13. Gaurav Kumar Gupt, Mr. Jitendra Singh, "Truth of D-DoS Attacks in MANET", vol. 10, issue 15, GJCST 2010.
14. Humaira Ehsan, Farrukh Aslam Khan, "Malicious AODV: Implementation and Analysis of Routing Attacks in MANETs", in proceedings of IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, 2012.
15. Irshad Ahmed Sumra, HalabiHasbullah, J. Ab Manan Mohsan Iftikhar, Iftikhar Ahmad, Mohammed Y Aalsalem "Trust Levels in Peer-to-Peer (P2P) Vehicular Network"2011 IEEE.
16. Irshad Ahmed Sumra, Halabi Hasbullah, Jamalul-lail Ab Manan, "VANET Security Research and Development Ecosystem", 2011 IEEE.
17. Irshad Ullah, Shoaib Ur Rehman, Analysis of Black Hole attack On MANETs Using different MANET Routing Protocols, School of Computing/ Blekinge Institute of Technology, June 2010,
18. Jaya Jacob et. al, " Performance Analysis and Enhancement of Routing Protocol in Manet", vol. 2, issue 2, pp. 323-328, IJMER, 2012.
19. João A. Dias, João N. Isento, Vasco N. G. J. Soares, Farid Farahmand, and Joel J. P. C. Rodrigues "Testbed-based Performance Evaluation of Routing Protocols for Vehicular Delay-Tolerant Networks" (2011 IEEE).
20. Lamyaa M.T. Harb, Dr. M. Tantawy, Prof. Dr. M. Elsoudani, "Performance of Mobile Ad Hoc Networks under Attack", pp. 1201-1206, IEEE 2013.
21. Linyang Sheng, Jingbo Shao, Jinfeng Ding, " A Novel Energy-Efficient Approach to DSR Based Routing Protocol for Ad Hoc Network", in proceedings of The International Conference on Electrical and Control Engineering, 2010.
22. Lu Chen, Hongbo Tang, Junfei Wang, "Analysis of VANET Security Based on Routing Protocol Information", 2013 Fourth International Conference on Intelligent Control and Information Processing (ICICIP) June 9 – 11, 2013, Beijing, China pp.134-138.
23. M. Khabazian, M. K. Mehmet Ali, "A Performance Modeling of Vehicular Ad Hoc Networks (VANETs)", 2007 IEEE.
24. Marco Tiloca, Domenico De Guglielmo, Gianluca Dini and Giuseppe Anastasi, "SAD-SJ: a Self-Adaptive Decentralized solution against Selective Jamming attack in Wireless Sensor Networks", ETFA, vol. 18, pp. 1-8, IEEE, 2013.
25. Md. Monzur Morshed, Md. Rafiqul Islam, "CBSRP: Cluster Based Secure Routing Protocol", IACC, vol. 3, pp. 571-576, IEEE, 2013.
26. Mina Vajed Khiavi1, Shahram Jamali2, Sajjad Jahanbakhsh Gudakahriz3, " Performance Comparison of AODV, DSDV, DSR and TORA Routing Protocols in MANETs ", International Research Journal of Applied and Basic Sciences, vol. 3, no. 7, pp. 1429-1436, 2012, ISSN 2251-838X.
27. Muhammad A. Javed and Jamil Y. Khan "A Geocasting Technique in an IEEE802.11p based Vehicular Ad hoc Network for Road Traffic Management". (2010).

28. N. Suganthi, V. Sumathy, "Energy Efficient Key Management Scheme for Wireless Sensor Networks", vol 9, issue 1, pp. 71-78, INT J COMPUT COMMUN, 2014.Ivan Damgård, Thomas P. Jakobsen, Jesper Buus Nielsen, and Jakob I. Pagter, "Secure Key Management in the Cloud", Cryptography and Coding Lecture Notes in Computer Science, volume 8306, pp. 270-289, Springer, 2013.
29. P.Kuppusamy, Dr.K.Thirunavukkarasu," A Study and Comparison of OLSR, AODV and TORA Routing Protocols in Ad Hoc Networks", pp. 143-147, IEEE, 2011.
30. Patrice Seuwou, Dilip Patel, Dave Protheroe, George Ubakanma "Effective Security as an ill-defined Problem in Vehicular Ad hoc Networks (VANETs)".
31. Ramaswamy Chandramouli, Michaela Iorga, Santosh Chokhani, "Cryptographic Key Management Issues & Challenges in Cloud Services", Computer Security Division Information Technology Laboratory, NIST, 2013.
32. Richa Agrawal, Rajeev Tripathi, Sudarshan Tiwari , " Performance Evaluation and Comparison of AODV and DSR Under Adversarial Environment", in proceedings of The International Conference on Computational Intelligence and Communication Systems, 2011.
33. Samir R. Das et. al, "Comparative Performance Evaluation of Routing Protocols for Mobile, Ad hoc Networks", ICCCN, pp. 153-161, IEEE, 1998.
34. Songqiao Han, Yong Zhang, "Design and Implementation of Service Composition Protocol Based on DSR", in proceedings of The 11th International Conference on Parallel and Distributed Computing, Applications and Technologies, 2010.
35. Steffen Moser, Simon Eckert and Frank Slomka "An Approach for the Integration of Smart Antennas in the Design and Simulation of Vehicular Ad-Hoc Networks" 2012 IEEE.
36. Tariq A. Alahdal, Saida Mohammad, "Performance of Standardized Routing Protocols in Ad-hoc Networks", ICCEEE, vol. 1, pp. 23-28, IEEE, 2013.
37. Yi Qian, Kejie Lu, and Nader Moayeri "Performance Evaluation of a Secure Mac Protocol for Vehicular Networks" (2008 IEEE).
38. Yogesh Chaba, Yudhvir Singh , Manish Joon, " Simulation Based Performance Analysis of On-Demand Routing Protocols in MANETs", in proceedings of The Second International Conference on Computer Modeling and Simulation, 2010.
39. Zongwei Zhou, Jun Han, Yue-Hsun Lin, Adrian Perrig, Virgil Gligor, "KISS: Key it Simple and Secure Corporate Key Management", Trust and Trustworthy Computing Lecture Notes in Computer Science, volume 7904, pp. 1-18, Springer, 2013.
40. Haowen Chan, Adrian Perrig, and Dawn Song. Random key predistribution schemes for sensor networks. In SP '03: Proceedings of the 2003 IEEE Sympo- sium on Security and Privacy, page 197, Washington, DC, USA, 2003. IEEE Computer Society.
41. Haowen Chan, Virgil D. Gligor, Adrian Perrig, and Gautam Muralidharan. On the distribution and revocation of cryptographic keys in sensor networks. IEEE Trans. Dependable Sec. Comput., 2(3):233–247, 2005.
42. Douglas R. Stinson. Combinatorial Designs: Construction and Analysis. Springer-Verlag, 2004.
43. Laurent Eschenauer and Virgil D. Gligor. A key-management scheme for distributed sensor networks. In CCS '02: Proceedings of the 9th ACM con- ference on Computer and communications security, pages 41–47, New York, NY, USA, 2002. ACM.