IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 7, July 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.542

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907232 |

A Novel Home Security Mechanism using Paired Key for Sensor to Cloud Communications

Kirandeep Kaur, Sarbjeet Kaur,

Department of Computer Engineering, AIET, Faridkot, Punjab, India

Department of Computer Engineering, AIET, Faridkot, Punjab, India

ABSTRACT: The house security models are gaining the popularity over the years, and adding more active systems for the house security. The prominent home security players are utilizing the cloud based centralized monitoring based update systems for the incorporation of the high-end security. The cloud based security models for homes requires the special level of security for the integration of the privacy and integrity among the data propagation. The data propagation security can be realized using the effective authentication mechanism. In this paper, the proposed model has been designed with the paired key mechanism. The paired key mechanism is being used for the sharing of the security data among the both ends of the home security communications. The proposed model has been equipped with the stronger encryption model by incorporating the advanced encryption standard (AES) for the data encryption for the privacy protection among the connection setup between the home security sensors and the cloud based home monitoring system. The proposed model has undergone the detailed performance evaluation in order to understand the effectiveness of the security scheme. The proposed model has been found effective and secure in the terms of the evaluated parameters. The proposed model has been improved by nearly 5-10% in all of the paradigms analyzed under the performance evaluation survey.

KEYWORDS: Home security sensor, invading analysis sensor, breach sensor, sensor security, sensor cloud secure model.

I. INTRODUCTION

There's no shortage of predictions regarding however the net of Things (iot) goes to revolutionize aid by dramatically lowering prices and up quality. However what we're seeing at Freescale is that it's already doing that. In these ways in which, iot-driven systems area unit creating it doable to radically scale back prices and improve health by increasing the supply and quality of care. We'll begin with associate introduction to the internet of things— still a comparatively new concept—but the one equipped with the growing paradigm of the smart apps for the variety of the applications. Good city is that the merchandise of accelerated development of the new generation information technology and knowledge-based information sharing among the internet, communication establishments, network broadcasts and meta-heuristic sensors networks where the web ofiot technology as its core. The integration of the services in the IoT services requires the high order information sharing over the wireless channels, which must be secured before being propagated over the communication channels. The smart services along with the smarter security and balanced architecture play the vital role in the establishment of the smart services associated with the variety of the services.The Internet of Things is regarding setting up sensors (RFID, IR, GPS, device scanners, etc.) For everything, and connecting them to internet through specific protocols for information exchange and communications, thus on understand intelligent recognition, location, tracking, observation and management. With the technical support from IoT, sensible city ought to have three choices of being instrumented, interconnected and intelligent. Entirely then a wise city area unit typically formed by human activity of those intelligent choices at its advanced stage of IOT development.

II. LITERATURE REVIEW

Kumar, Adarsh et. Al. has worked upon simulation and analysis of authentication protocols for mobile based internet of Things (MIoT). This work proposes one bar circular topology based mostly authentication protocol for MIoT. This protocol helps in authenticating the mobile devices for constructing secure network. The planned protocol is sculptured mistreatment Alloy model. Delay analysis shows that construction of secure network is feasible with most delay of

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907232 |

zero.91 msec. Node will enter or leave the network with minimum of zero.13 and most of zero.20 msec. Further, Zone Routing Protocol (ZRP) is taken into account to be the simplest protocol for constructing a secure network. Lee, Jun-Ya et. Al. has planned a light-weight authentication protocol for net of things. During this paper, the authors have planned associate degree encoding technique supported XOR manipulation, rather than advanced encoding like mistreatment the hash perform, for anti-counterfeiting and privacy protection. The sweetening of the safety is represented and hardware style methodology is additionally incontestible. Abomhara, Mohamed et. Al. has given the study on security and privacy within the net of Things: Current standing and open problems. As IoT systems are omnipresent and pervasive, variety of security and privacy problems can arise. Credible, economical, economical and effective security and privacy for IoT are needed to confirm precise and correct confidentiality, integrity, authentication, and access management, among others. During this paper, the IoT vision, existing security threats, and open challenges within the domain of iot are mentioned. The present state of analysis on IoT security needs is mentioned and future analysis directions with relevancy IoT security and privacy are conferred. Ali, Syed Taha et. Al. has worked on the authentication of lossy information in body-sensor networks for cloud-based care watching. During this paper, the authors have planned a light-weight sturdy authentication theme. They need analyzed and validate a sensible approach for his or her analysis to develop the authentication theme. The authors have aimed their analysis for care watching systems. The planned theme has been lower on price and loss-resilient. The new theme has been tried to effective on virtually ninety nine of knowledge and it's supplementary as low as five-hitter overhead. Khan, Farrukh Aslam et. Al. has planned a cloud-based care framework for security and patients' information privacy mistreatment wireless body space networks. The authors have conferred a secure cloud-based mobile care framework mistreatment WBAN clusters. The authors have developed a multi-biometric based mostly key generation theme for WBAN clusters. They need conjointly worked upon electronic medical records and secured them mistreatment the authentication theme supported the key sharing method. The analysis and analysis shows that the planned multi-biometric based mostly mechanism provides important security measures because of its extremely economical key generation mechanism.

III. EXPERIMETNAL DESIGN

The proposed model is based upon the data propagation security between the house panel and cloud panel. The proposed model has been perfectly designed for the establishment of the security among the house monitoring procedure. The incorporation of the authentication and key encryption has been performed to fulfill the requirement of the security among the house sensor security. The authentication based security model utilizes the paired key mechanism for the purpose of authentication between the house sensor, remote panel and the cloud based monitoring panel. The advanced encryption standard (AES) based upon the 128-bit block size along with the 128-bit long key data has been proposed for the robustness of the authentication security model. The following algorithm defines the working of the proposed model.

Algorithm 1: Main IoT authentication Algorithm

1. *Fetch command signal from house panel → cSig*
2. *Count the number of requests being propagated under the one final request → cCount*
3. *Encrypt the string data in the command URL → hCommands*
4. *Setup the secure connection with the cloud based house monitoring server*
5. *The request acknowledgement is returned by the cloud server*
6. *When the acknowledgement is received*
    a. *Prepare and Propagate the device details*
        i. *Device ID*
        ii. *Security PIN*
        iii. *Current status of device*
    b. *Do the following*
        i. *If the provided information is matched successfully*
        ii. *The cloud sends the accepted acknowledgement (ACACK)*
    c. *Terminate the connection*
7. *When the ACACK is received*
    a. *House sensor prepare the data*
    b. *Encrypt the data using the AES*
    c. *Transmit this to the cloud server*
8. *Cloud server receives the data*
9. *Decrypts the data*

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907232 |

10. *Sensor node awaits till the next update is triggered*
11. *When the change is reported*
12. *The data update procedure is restarted*

1. RESULT ANALYSIS

The proposed model has been evaluated for the performance in the terms of various performance parameters. The proposed model has been analyzed for the level of security, time complexity and memory consumption. The proposed model has undergone the multi-layered security analysis approach in order to estimate the strength of the authentication model from the different aspects.

3.1 Time based analysis

The key verification time and key transfer times have been analyzed in order to understand the time based complexity of the proposed model in the two-way authentication using the proposed model. The proposed model has been recorded with very less time, which shows the effectiveness of the proposed model while propagating the authentication data.

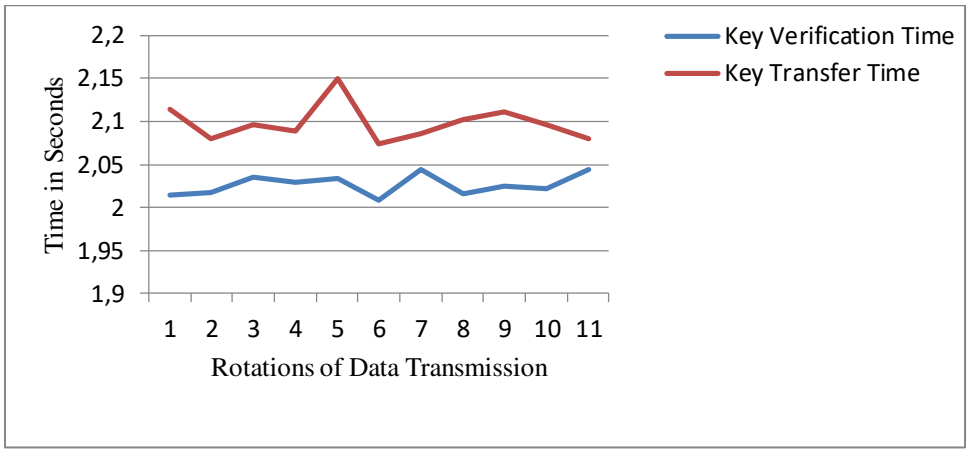

Figure 4.1: The analysis of the time complexity based upon the two-way authentication

The figure 4.1 shows the key transfer and key verification time values obtained from the proposed model simulation. The proposed model has been recorded with the key exchange interval nearly around 2 second, when computed on the average. The average time of 2.01 seconds has been recorded for the key transfer and 2.02 seconds for the verification decision and sends the acknowledgement backs to the client device.

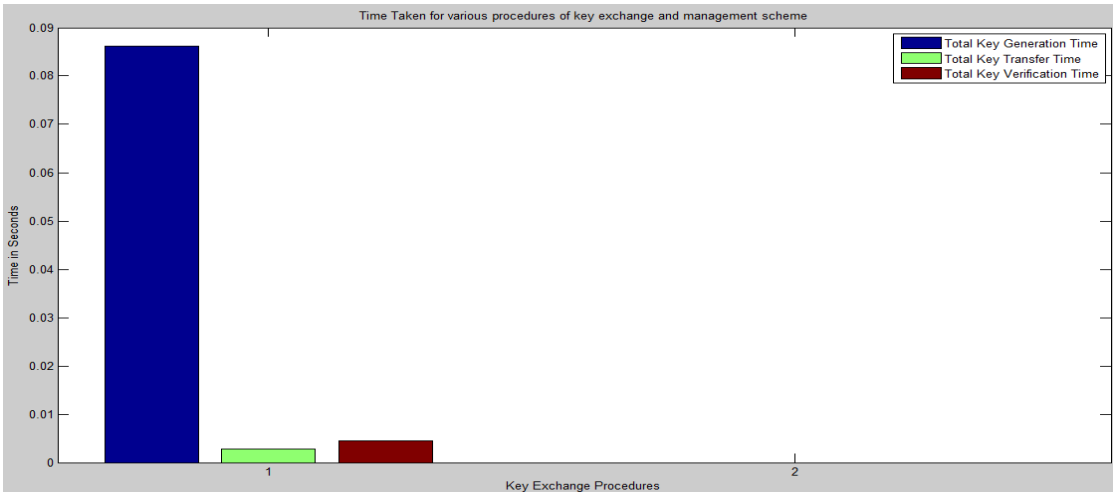

Figure 4.2: The average value based analysis of the time-based factors

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907232 |

The figure 4.2 shows the average results of the key time analytical factors. The proposed model has been recorded with very less key transfer time and key verification time on an average, when the run the simulation for the longer times. The key generation time is higher but it takes place once in every session, which can justify the performance of the proposed model.

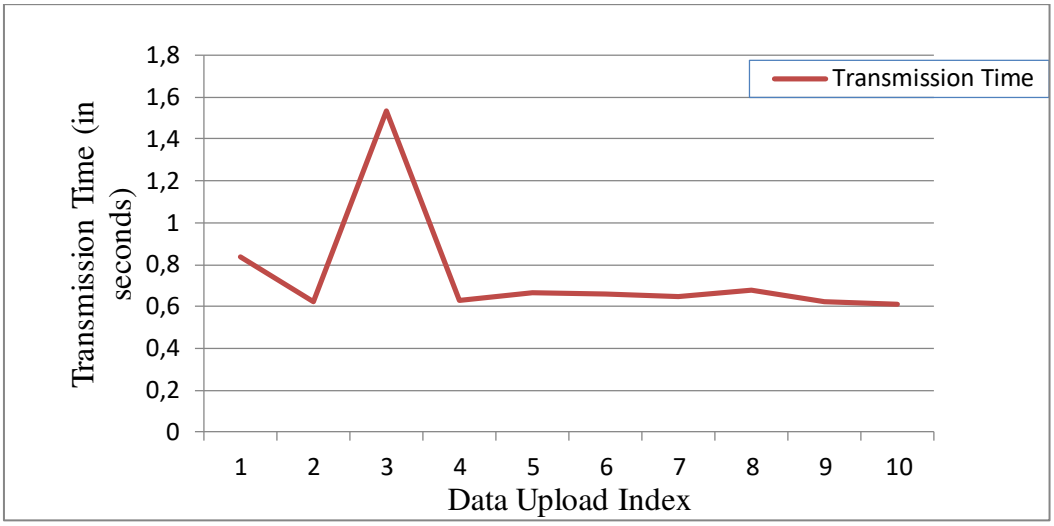

Figure 4.3: Overall transaction time for data communication between the cloud and client sensor

The overall transaction time has been recorded to estimate the overall time cost for each transaction, once the connection is established and the key tables are kept shared between the source sensor and cloud environment. The average transaction time of nearly 0.6 seconds shows the robust performance of the proposed model.

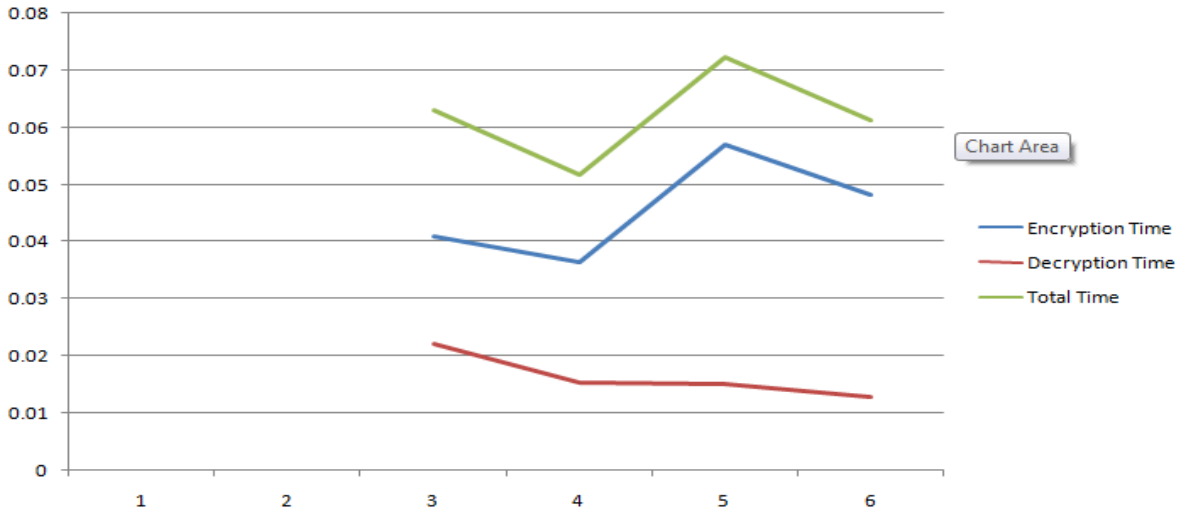

Figure 4.4: Encryption algorithm's time analytical analysis

The encryption algorithm has been utilized for the robustness of the security among the communication between the house security sensor and the remote panel and the house security sensor and the cloud platform. The proposed model has been deeply analyzed for the time complexity factor for the encryption of the key data alone. The AES encryption algorithm has been shown the very low overhead, which has been remained nearly at 0.06 seconds on an average.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907232 |

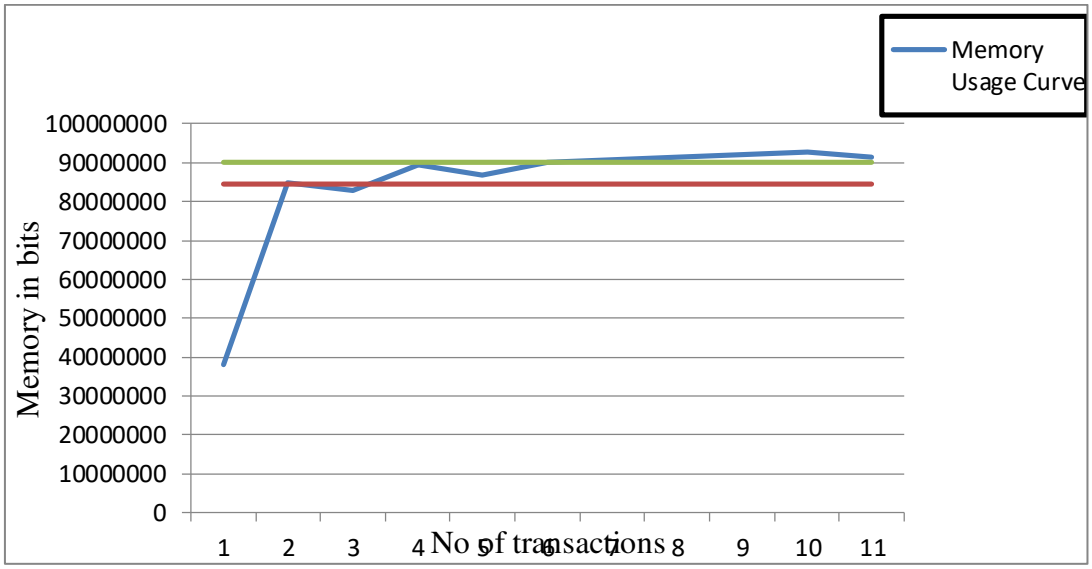

Figure 4.5: memory consumption based analysis

The analysis of the proposed model based upon the memory consumption has been performed in order to read the processing cost of the proposed authentication model over the computational resources. The proposed model has been recorded with the lower memory consumption, which shows the efficiency of the proposed model.

IV. CONCLUSION

The authentication schemes protect against the malicious injections in the given network. The proposed model has been designed by using the layered security model for the fulfilling of the semantic gap in the security among IoT networks. Meanwhile, some important concepts related to information sharing and integration in IoT clouds discussed and analyzed the arising security and privacy issues in access and management of electronic house monitoring records. Then the security reference model for managing security issues in IoT clouds is presented, which highlights three important core components in securing an house monitoring record on the cloud servers. Finally, the development of the proposed electronic home record security reference model through a use-case scenario is illustrated along with corresponding security countermeasures and possible security techniques. 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.

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).Authenticationoflossy datainbody-sensor networksforcloud-basedhealthcaremonitoring.FutureGenerationComputerSystems, 35,80-90.
5. Khan,F.A.,Ali,A.,Abbas,H.,&Haldar,N.A.H.(2014). ACloud-basedHealthcare Framework for Security and Patients' Data Privacy Using Wireless Body Area Networks. Procedia ComputerScience, 34, 511-517
6. Peng,X.,Zhang,H.,&Liu,J.(2014).AnECGCompressedSensingMethodofLowPowerBodyAreaNetwork.TELKOMNIKAIndonesianJournalofElectricalEngineering, 12(1),292-303.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907232 |

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. Asma Tuteja et. al, "Comparative Performance Analysis of DSDV, AODV and DSR Routing Protocols in MANET using NS2", ICACE, pp. 330-333, IEEE 2010.
9. Fuad A. Ghaleb, M. A. Razzaque, Ismail FauziIsnin "Security and Privacy Enhancement in VANETs using Mobility Pattern" (IEEE,2013).
10. 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.

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 7.542

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details