# Multi-Column Key Authentication for Healthcare Systems (MCKA-HS) over the Cloud-Sensor Communications

**Shilpa Kansal[1] Navpreet Kaur[2]**
[1,2]Department of Computer Science & Engineering
[1,2]Punjabi University Regional Centre for Information Technology and Management, Mohali, Punjab, India

*Abstract*— The healthcare networks have grown the popularity in the recent years. The healthcare networks suffer from the major problem of security over the small computational powered wireless healthcare sensors. In this paper, the major focus has been kept on the development of the lightweight but secure and robust authentication scheme. The proposed healthcare authentication model is based upon the multi-column key computations in the complex manner for the preparation of the robust and secure authentication scheme. The proposed authentication model has been designed for the higher order robustness in the cloud based healthcare network security architecture for the communication established between the wireless healthcare sensor (WHS) and the cloud healthcare server (CHS). The proposed multi-column authentication is based upon the complex key sharing between both of the ends over the healthcare networks to provide the higher privacy to the healthcare data. The proposed model has been designed using the equation driven program using the mathematical computational modules for key data generation and verification over the both ends of the healthcare communication. The CHS propagates the other set of the equation programming using the various mathematical methods collaborated to handle the key verification procedure. The key sharing method is supervised by the transmission module which circulates the key data between both of the nodes in the authentication pair. The proposed model has been evaluated on the basis of various performance parameters for the performance evaluation. The experimental results have clearly shown the robustness of the proposed model in comparison with the existing model.

***Key words:*** Adaptive Healthcare Security, Healthcare Authentication, MCKA-HS, Wireless Healthcare Sensors (WHS)

## I. INTRODUCTION

Healthcare is one of the major concern, since it involves the quality of life of an individual. It is always better to prevent an illness than to treat it, so individual monitoring is required as a periodic activity. The aging population of developed countries presents new challenges to healthcare systems, namely with elderly people living on independent senior housing. Traditionally, health monitoring is performed on a periodic check basis, where the patient must remember its symptoms as the doctor performs some check and formulates a diagnostic, then monitors patient progress along the treatment. However, some symptoms only manifest themselves in daily activities, where an individual may feel some pain or discomfort. Healthcare applications of wireless sensor networks allow in-home assistance, smart nursing homes, clinical trial and research augmentation. In-home healthcare becomes mandatory for various diseases, providing memory enhancement through medicine reminders, mental stimulation through sounds or images of object's location, control over home appliances, medical data lookup, and emergency situations. Before describing and surveying medical applications for healthcare. This paper focuses on several challenges and general aspects that characterize this kind of technologies.

Wireless sensor network (WSN) typically consists of a collection of sensors with their own power supply, wireless communication, data storage, and data processing capability. WSN's are deployed to sense and monitor the physical world by providing real time information. These network devices are self-governed. The sensor nodes of wireless network communicate with each other via radio signal in the absence of physical network. The nodes of wireless network consist of finite memory, sensor, a radio transceiver & sufficient power source. The information provided by WSN have data integrity as the data transfer by the sender is not modified on the path from sender to receiver. Confidential information is anticipated in wireless network it denotes particular information must be prevented from entrusted third party. The nodes of wireless sensor network are vulnerable to attacks. WSN are endangered with security attacks that ows broadcast nature over transmission medium. Each sensor node in sensor network has a microprocessor with limited processing capability, energy supply and bandwidth and a small amount of memory for signal processing.

Major applications using WSNs include: Traffic monitoring, Habitat monitoring, Forest fire detection, Natural disaster prevention, Healthcare monitoring, Mood-based services, Positioning and Animal tracking, Entertainment, Logistics, Transportation, Home and Office, Industrial and Military monitoring. There has been an increasing use of sensor networks for life critical applications such as monitoring patients in Hospitals. These applications make it important to have a good security infrastructure for sensor networks called as wireless health sensors (WHS). The deployment of these networks in hospital applications and the limited security level, make the design of a security protocol very challenging. Health care applications enable people with certain medical conditions to receive constant monitoring through sensors. The authentication scheme based healthcare data privacy algorithm in the base paper has been proposed. The existing authentication scheme is based on secure key exchange based on Diffie-Hellman key exchange algorithm.

Wireless Body Area Networks are various wearable or implanted electronic devices that provide doctors the real time data about patients anywhere within or outside the medical center as that is made available online. These networks are composed of wireless health sensors (WHS's) that transmit their ID or sensor data to the gateway. The network of sensors is kept on or close to the

 

surface of patients body or may even plated into the tissue so that patients physiological data can be achieved regardless of patients location, his health is monitored continuously. Sensors can be transceivers or receivers depending on the bandwidth of data to be collected. These sensors require accuracy, low power of signal processing and wireless capabilities and must be robust against various interferences in environment. Such approach may lead to a multi-tiered architecture, with lightweight mobile computers and smart sensors in conjunction with more powerful computational devices

Cloud Healthcare Server, the cloud platform networks are growing across the world and positive results are being derived from such platform networks. Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over the network (mainly the Internet). Cloud has abundant processing power, large amount and long term data storage which can be scaled according to application needs. The cloud based platform service becomes more efficient as a higher volume of resources is always available for the applications hosted on the clouds, which can be utilized when the computational overhead increases due to the number of user requests or the internal application process execution. The proposed system focuses on collection of patient's data and generates alert to care takers, doctors so that immediate action can be taken in case of emergencies. The data is then stored in Cloud so that data can be accessed via Internet from anywhere anytime.

The platform network consists of wireless body sensors for live health monitoring and the platform database management servers. Instead of attaching sensors to medical equipments, wearable sensors are attached to human body which continuously monitor and collects data regarding the blood pressure rate, heartbeat, fall detection, etc.

In our proposed model, system utilizes mobile devices to display and transmit physiological signals such as the ECG signal and heart beat rate. Then, the health information is collected, synchronized, and shared instantaneously over the Web server through Wi-Fi or a data network, as any heart attack or heart disease must be diagnosed immediately. The raw health data are stored in cloud storage to enable professional medical personnel to access and analyze0 the monitoring results, providing appropriate care services. Using the embedded Web server and dynamic Web page technology, the health status is displayed on a Web page; family members can check the medical records at any convenient time. The major problem of the cloud based network services lies in the security of the platform applications.

Healthcare Authentication, the proposed scheme is specially proposed for wireless platform sensor networks. The wireless user nodes are battery operated devices, hence, having limited power sources. The platform sensors or sensor networks sends data to the platform record management services via long distance wireless communication channels such as cellular networks or radio networks. The communication between the wireless body sensor and cloud based platform service passes from many insecure network ingress or egress points, where there is higher risk of the communication data being exposed to the hackers. To protect the communication we are proposing a novel key exchange methods based upon the randomized key generation and management policy as the major improvement for the diffie-hellman scheme. Our scheme does not rely upon the key reversal or re-computational process, but is robust and rigid in nature, which does not allow any of the key guessing attacks. Such attacks do not let the sensor device to become hostile to the hackers and do not expose any information to the hackers. The paper is concluded with a brief analysis on the possible countermeasures to prevent security attacks.

## II. LITERATURE REVIEW

Hernandez-Rasmos, Jose L. et. al. [9] Proposed authentication and authorization scheme which is based on Deffie-Hellman along with Advanced encryption standard(AES) for the security of IoT sensor devices which is integrated with security framework Architectural Reference Model (ARM).

Ali, Syed Taha et. al. [11] has worked on the authentication of lossy data in body-sensor networks for cloud-based healthcare monitoring. In this paper the author introduces low cost and robust authentication scheme for healthcare monitoring devices. Develops optimizing framework to maximize data verification for given overhead and loss environment. Validates the scheme by verifying maximum percent of data can be authenticated with low overheads and at low cost.

Abderrahim, Bourouis et. al. [7] In this paper author uses Wireless Body Area Networks(WBANs) and smart phone application in order to access patients current data by using various wearable monitoring devices. Purposed a new architecture which collects and sends data to the cloud through GPS system.

Jun, Zhou et. al. [2] purposes a flexible model about preserving patients privacy and authentication scheme (PSCPA). Three levels of security and privacy have been released by resisting denial of service attacks. Authorized persons data can access patients personal data by their ID.

Abomhara, Mohamed et. al.[16] discuss the Current status and open issues regarding the security and privacy in the Internet of Things. Author tries to overcome various challenges like security and privacy issues such as authentication authorization of entities are introduced, design of architecture standards, categorizing IoT technologies and difficulties.

Patel Maulin et. al. [5] discusses about various applications and challenges regarding body area networks. Discussed about the design of wireless system and challenges like scalability, security, privacy, energy efficiency.

Rahmani, Amir-Mohammad et. al. [14] has worked on a prototype of smart e-health gateway and brings improvement in the challenges like scalability, energy efficiency, reliability, interoperatatability in the ubiquitous systems. Demonstrated through data flow process new introduced UT-GATE. Described their architecture into three main components Medical Sensor Network, Smart e-Health Gateway, Back-End System.

Kumar, Adarsh et. al.[3] has worked upon simulation and analysis of authentication protocols for mobile Internet of Things (MIoT). This work purposes authentication protocol for MIoT named single bar circular topology which helps in constructing a secure network for

 

authenticating mobile devices. Radio frequency identification (RFID) based devices communicate with each other using various routing protocols. As in this zone routing protocol which is modelled using alloy model proved as the best for constructing a secure network with limited delay.

Hassanalieragh, Moeen et. al. [4] reviewed the availability of health data. Discussed about the opportunities and challenges related to acquiring, analyzing and visualizing remote health monitoring.

## III. Experimental Design

The existing model is based upon the healthcare security system authentication and key aggregation (HSS-AKA) and has been improved as the efficient HSS-AKA (also EHSS-AKA). The EHSS-AKA model has been comprised of the security model to protect against the information disclosure vulnerabilities and man in the middle attacks in the healthcare applications. The existing system is multi-column paired-key based authentication model with the advanced encryption standard. The existing model has been made to share four messages for one round of authentication. It utilizes the simple password exponential key exchange (SPEKE) model of the base model implementation and has been developed with certain defined improvements.

The proposed model is Multi-Column Key Authentication for Healthcare Systems (MCKA-HS). This model has been designed as the robust security architecture for the healthcare surveillance systems connected via 2G, 3G, 4G, WLAN, WiMAX, Zigbee etc. The proposed model is the flexible authentication scheme for the healthcare surveillance using the complex key model in this model. The proposed model has been developed as the complex key architecture where the multiple columns based key model has been used for the secure authentication over the healthcare services established between the patient and cloud based healthcare services. The equation driven mathematical programming has been incorporated for the purpose of key data generation over the node with the data origination. The receiver node propagates another set of the mathematical programming written to satisfy the procedure of key verification. The key sharing method is supervised by the transmission module which circulates the key data between both of the nodes in the authentication pair.

For authentication purpose, we are using a table with 5 columns and multiple rows in which the first 3 columns (i.e. a, b, c) are used for query key generation and the last 2 columns (i.e. d, e) are used for reply key building. The table is shown below:

| A | b | c | d | e |
|---|---|---|---|---|
| | | | | |

Table 1: Key Table

### *A. Query Key Generation*

Query key=
round(log10(sin(a)*cos(b)*tan(c))*887000+(a*b*c))

### *B. Reply Key Generation*

Reply key=
round(log10(sin(d), atan2(d,e)*180/pi)*347100)

### *C. Main Key Generation Policy*

*1) Algorithm: Key Authentication Sequence for Healthcare Systems*

- Wireless Healthcare Sensor (WHS) initializes the connection setup and forwards the request cloud healthcare server (CHS)
- The cloud healthcare server (CHS) base station asks for the pre-shared information
- WHS replies with the pre-shared information
- If CHS verifies the pre-shared information phase
  - Initial communication phase is completed

*2) Main Algorithm*

- The CHS infuses the multi-column keys to prepare the query key.
- The query key is encrypted using the AES algorithm.
- The query key is forwarded to the WHS.
- The WHS prepares the reply key by verifying the query key column data and marks the reply key rows.
- The reply key is prepared by infusing the multiple keys information in the marked columns.
- The reply key is encrypted using the AES algorithm.
- The reply key is forwarded towards the CHS
- The CHS verifies the query key against the reply and prepares the decision.
- If the verification decision is successful
  - The healthcare data exchange begin between the patient and cloud based healthcare server
  - Initialize the timer
- Otherwise
  - Refuse the connection to the WHS
- If 9(a) successful
  - When the timer gets expired, GOTO step 1

## IV. Result Analysis

Projected resources: The projected resource has been evaluated for the measurement of the utilization of the resources over the given cloud healthcare network environment in the proposed model simulation. The high performance is indicated by the lower value of the projected resources computed from the simulation environment and higher value indicates the lower performance. MCKA-HS has been considered better than EHSS-AKA as it has been measured with the lower value for projected resources over the given simulation scenario of healthcare network. The detailed result evaluation has been described below:

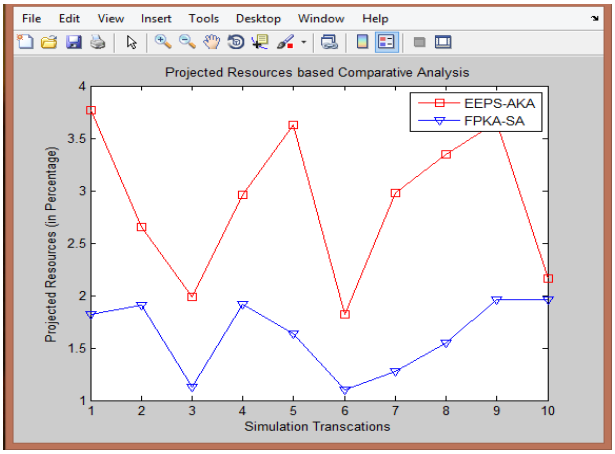


Fig. 1**:** Projected resources based graph for scenario 1

 

### *A. Entropy*

The key efficiency, size of population and the uniqueness of the entities in the given key table is measured by using the entropy parameter. The unique data decreases the risk of key exposure to the hacking attempts, which has been strongly observed from the proposed model simulation. The consistently high entropy justifies the strength of the security of the healthcare networks. The detailed results for entropy can be seen below:

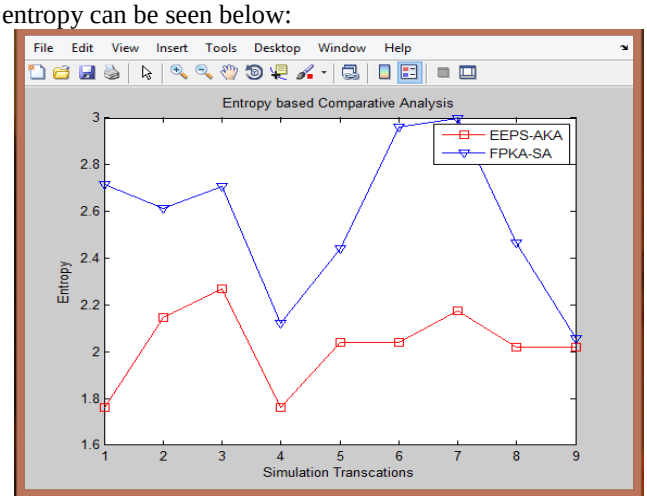


Fig 2: Entropy based graph for scenario 1

### *B. Comparative Analysis for scenario 1*

The comparison of the evaluated results has been performed over the results obtained from the existing and proposed models. The performance evaluation has been performed on the basis of projected resources and entropy. MCKA-HS has been proved itself as the better model than EHSS-AKA. MCKA-HS has been proved to be efficient than EHSS-AKA on the basis of both the performance parameters.

| Key Index | EHSS-AKA | MCKA-HS |
|---|---|---|
| 1 | 3.7667 | 1.8164 |
| 2 | 2.6499 | 1.9063 |
| 3 | 1.9840 | 1.1250 |
| 4 | 2.9604 | 1.9141 |
| 5 | 3.6282 | 1.6328 |
| 6 | 1.8221 | 1.0977 |
| 7 | 2.9796 | 1.2773 |
| 8 | 3.3467 | 1.5469 |
| 9 | 2.1651 | 1.9648 |

Table 2**:** Projected Resources based comparison for scenario 1

| Key Index | EHSS-AKA | MCKA-HS |
|---|---|---|
| 1 | 1.7632 | 2.7158 |
| 2 | 2.1466 | 2.6115 |
| 3 | 2.2706 | 2.7054 |
| 4 | 1.7632 | 2.1222 |
| 5 | 2.0412 | 2.4402 |
| 6 | 2.0412 | 2.9598 |
| 7 | 2.1762 | 2.9963 |
| 8 | 2.0207 | 2.4678 |
| 9 | 2.0207 | 2.0544 |

Table 3: Entropy based comparison for scenario 1

The entropy of the proposed key scheme has been tested over the proposed key schemes. The entropy parameter measures the uniqueness of the keys during the key selection mechanism. The MCKA-HS adds the additional robustness in the proposed security scheme associated with the key exchange for healthcare networks. The result of the proposed model has been observed nearly double than the existing model, which can be clearly indicated by the following table.

| **Entropy** | **S1:N1** | | **S2:N5** | | **S3:N10** | |
|---|---|---|---|---|---|---|
| | **EHSS-AKA** | **MCKA-HS** | **EHSS-AKA** | **MCKA-HS** | **EHSS-AKA** | **MCKA-HS** |
| **Average** | 2.0207 | 2.4678 | 2.0131 | 2.6344 | 2.0712 | 2.7662 |
| **Minimum** | 1.7632 | 2.0544 | 1.6090 | 2.1550 | 1.7707 | 1.9910 |
| **Maximum** | 2.2706 | 2.9963 | 2.4393 | 3.1638 | 2.3884 | 3.2897 |

Table 4: Entropy comparison between EHSS-AKA and MCKA-HS

| **Projected Resources** | **S1:N1** | | **S2:N5** | | **S3:N10** | |
|---|---|---|---|---|---|---|
| | **EHSS-AKA** | **MCKA-HS** | **EHSS-AKA** | **MCKA-HS** | **EHSS-AKA** | **MCKA-HS** |
| **Average** | 2.6499 | 1.5469 | 13.3108 | 7.7344 | 26.4594 | 15.4688 |
| **Minimum** | 1.8221 | 1.0977 | 7.8656 | 5.4883 | 15.0027 | 11.2500 |
| **Maximum** | 3.7667 | 1.9648 | 19.7488 | 9.8242 | 38.6813 | 19.6484 |

Table 5: Projected Resources comparison between EHSS-AKA and MCKA-HS

## V. CONCLUSION

The new MCKA-HS scheme has been primarily evaluated for the utilization of the resources while using the security algorithm over the 4G/LTE network. The utilization of the resources, measured in the form of projected resources has been recorded significantly lower than existing model, which clearly indicates the robustness of the proposed model. The following table (Table 4.3) indicates the robust performance of the proposed model. Additionally, the entropy parameter signifies the higher level of security in the MCKA-HS model than the existing model. The MCKA-HS model evaluation over the entropy has been described in the following table (Table 4.4). The proposed model has clearly proved the efficiency of the proposed model in comparison with the existing model. The experimental results have proved the proposed model as the clear winner for the healthcare authentication.

## REFERENCES

[1] Huan-Chao Keh, Chun-Che Shih, Kuang-Yi Chou, Yuan-Cheng, Cheng, Hsin-Kai Ho, Po-Yuan Yu and Nan-Ching Huang, "Integrating Unified Communications and Internet of M-Health Things with Micro Wireless Physiological Sensors" in Journal of Applied Science and Engineering, Vol. 17, pp. 319328, 2014.

 

[2] Zhou, Jun, and Zhenfu Cao. "PSCPA: Patient Self-controllable Privacy-preserving Cooperative Authentication in Distributed m-Healthcare Systems." in IACR Cryptology 2012.
[3] 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.
[4] Moeen Hassanalieragh, Alex Page, Tolga Soyata, Gaurav Sharma, Mehmet Aktas, Gonzalo Mateos, Burak Kantarci, Silvana Andreescu,"Health Monitoring and Management Using Internet-of-Things (IoT) Sensing with Cloud-based Processing: Opportunities and Challenges" in IEEE International Conference on Services Computing, IEEE, 2015.
[5] Maulin Patel , Jianfeng Wang, "Applications, challenges, and prospective in emerging body area networking technologies" in IEEE Wireless Communications PHILIPS RESEARCH NORTH AMERICA, vol 17, IEEE,Feb 2010.
[6] 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.
[7] Bourouis, Abderrahim, Mohamed Feham, and Abdelhamid Bouchachia. "A new architecture of a ubiquitous health monitoring system." in IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 2, March 2012.
[8] Carlos Oberdan Rolim, Fernando Luiz Koch, Jim Black and Claudio F. R. Geyer, "Health Solutions Using Low Cost Mobile Phones and Smart Spaces for the Continuous Monitoring and Remote Diagnostics of Chronic Diseases" in The Third International Conference on eHealth, Telemedicine, and Social Medicine, pp. 72-76,2011.
[9] Hernandez-Romas, Jose L.,Marcin Piotr Pawlowski ,Antonio J. Jara ,Antonio F. Skarmeta, and latif Ladid. " Towars a Lighweight Authentication and Authorization Framework for Smart Objects." Selected Areas in communications, IEEE Journal on 33, vol. 4, pp. 690-702, IEEE 2015.
[10] Giancarlo Fortino, Daniele Parisi, Vincenzo Pirrone, Giuseppe Di Fatta, "BodyCloud: A SaaS Approach for Community Body Sensor Networks"in BodyCloud: A SaaS Approach for Community Body Sensor Networks, Vol 35,pp. 62-79,Elsevier,June,2014.
[11] Ali S. T., Sivaraman, V.and Ostry, D. "Authentication of lossy data in body-sensor networks for cloud-based healthcare monitoring." in Future Generation Computer Systems, vol. 35,pp. 80-90, ELSEVIER,June 2014.
[12] Al Ameen,Liu J.,Kwak K. " Security and Privacy Issues in Wireless Sensor Neworks for Healthcare Applications." in Journal of Medical Systems,vol. 36,pp. 93-101,SPRINGER,Feb. 2010.
[13] Tina Francis, Dr. Muthiya Madiajagan, Dr. Vijay Kumar, "Privacy Issues and Techniques in E-Health Systems" in Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research. ,pp. 113-115,ACM, 2015.
[14] Amir-Mohammad Rahmani, Nanda Kumar Thanigaivelan, Tuan Nguyen Gia, Jose Granados, Behailu Negash, Pasi Liljeberg, and Hannu Tenhunen, "Smart e-Health Gateway: Bringing Intelligence to Internet-of-Things Based Ubiquitous Healthcare Systems" in 12th Annual IEEE Consumer Communications and Networking Conference (CCNC), IEEE, 2015.
[15] R.Kumar, Dr.M.Pallikonda Rajasekaran, "Raspberry Pi Based Patient Health Status Observing Method Using Internet Of Things"in International Conference on Current Research in Engineering Science and Technology, ICCREST, 2016.
[16] 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.

 