International Journal of Advance Research in Science and Engineering
Vol. No.6, Special Issue (01), September 2017, BVCNSCS 2017
www.ijarse.com
IJARSE
ISSN 2319 - 8354

Security Tool for Mining Sensor Networks

Bhaskar N[1], M.V. Ramanamurthy[2], S. Ramana[3]
[1]*Research Scholar, Computer Science, Rayalaseema University, Kurnool, A.P.*
[2]*Professor & BOS Chairman, Dept. of Mathematics and Computer Science, Osmania University, Hyderabad*
[3]*Research Scholar, Computer Science, Osmania University, Hyderabad, Telangana State*

ABSTRACT : *The purpose of the research paper is to provide the secured environment while mining sensors devices. The new trend in the present world scenario is remote sensor based devices. It makes the user to work easy by monitoring the devices from a remote location and control the functionality without human interference. The system works on WiFi enabled environment with proper security. It is easy to the user to control a device remotely. But the main problem is with security. This paper gives a security tool which is secured and having proper authentication and data encryption.*

Keywords: WIID - Wireless Infrared Intrusion Detection, GSM – Global Systems for Mobile Communications, RF - Radio Frequency, WSM – Wireless Sensor Networks, SMS – Short Message Service, Encryption, Intruders- who will enter system without your permission or access your system for some purpose and trying to attack and damage your system data.

I. Introduction

Objective: My research paper objective is to provide proper authentication, secured transmission of device details or information and intruders detection and prevention in the network. It provides an easy method of recognizing a device in WSN (Wireless Sensor Network), accessing from the secured environment and monitoring and preventing intruders in accessing the WSN from the network [1][2][3].

Now a day there are many applications coming up for different domain requirements. The applications could be network based, cloud based, remote based and application control by sensors. In this scenario, it is observed that the applications available for different purposes need the monitoring of the following aspects rather than regular user interfaces and backend support.

- Security
- Performance
- Storage space and data recovery

SECURITY: Security is critical for enterprises as well as small organizations of all sizes and in all industries. Weak security can result in open systems or data, either by a malicious threat actor or an unintentional internal threat. It causes the substandard security that are regulated by a separate organization or law.

PERFORMANCE

Software performance is one of the biggest challenges today in the present scenario of building any web or mobile based application. In the digital world today, every user wants a flow of information at a quick and the companies are focused on building a scalable and optimized software solution. How fast any software (web or mobile) responds to a user is one of the main criteria to analyze the success and user satisfaction of that software in the market. Therefore, building a scalable application is one of the challenging skills of software in the present market. The performance of software depends on the architecture and what technology is used in designing and implementation of the software. However, improving the performance of already developed large-scale applications can be a difficult task.

The parameters considered for the evaluation of system performance are:

- Memory Utilization
- Database
- Source Code

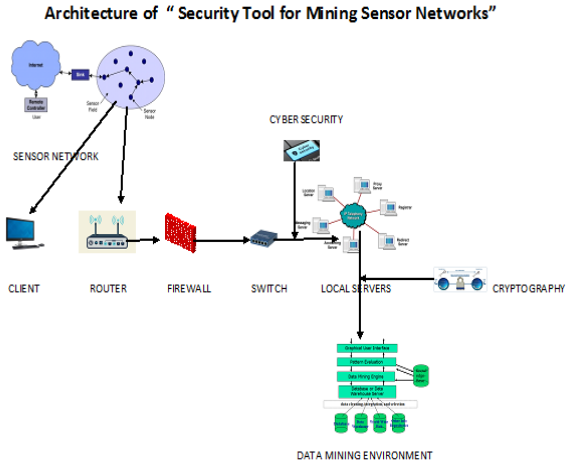
STORAGE SPACE and DATA RECOVERY

Storage Spaces enables cost-effective, highly available, scalable, and flexible storage solutions for business-application (virtual or physical) deployment [8]. Storage Spaces delivers safe and large volume of virtualization capabilities, which empower customers to use industry-standard

storage for single computer and scalable network application deployment. It is appropriate for a wide range of customers, including enterprise, cloud hosting companies, mobile apps developers with the platforms like Windows Server for highly available storage that can cost-effectively grow with demand.

II Problem Analysis

From the observation different papers, articles, publications on sensor devices, locating device in the network, accessing the devices by the user from a secured environment and in encrypted format of device content, following architecture and solution procedure is developed [10].



The proposed above architecture provides the following environment with their interaction [13][14].

- Data Mining Structure
- Local Network with Servers required
- Sensor network connecting devices through wireless
- Intermediate elements like Router, Firewall, Network Switch
- Cyber Security and Cryptography

III Solution Designed

After the detailed analysis of the literature survey and requirements, the problem identified is there is a need of security implementation, performance evaluation[11] and a solution suitable to access devices and data from remote location. It is also observed that, the solution should meet the needs of present technological era i.e. RFID, WI-FI, Cryptography models[12], and Protocols.

In this scenario, the proposed solution consists of the following procedures adopted by the author for clear understandability [4][6][7].

- Proposed algorithm
- Algorithm implementing environment
- Solution analysis with other available solutions

Algorithm Proposed

Assumptions: It is assumed that the pre-requisites like network environment, solution platform, hardware devices and sample data [9].

Step – 1:

Identify the devices required in the network for access. Each device in the network should be assigned with unique color code from color panel. Define the color code to each of the device available in the network for security purpose. We get unique set of colors, i.e., 16 777 216 (256^ 3) combinations of colors color code panel.

Step – 2:

Specify the device identity code of recognition in a single network topology and heterogeneous networks.

Step – 3 :

Each record of data base contains: Device Id, Color code selected with row and column value, Armstrong number uniquely identified for every instance, which is not allocated to other devices.

Step – 4:

User is allowed to change color code allocated to the device any time with proper authentication. Any device can be removed from the network at any time. The basic validation is that the color code assigned to any device should not be allowed to any device.

Step – 5:

Generate Armstrong number randomly every time for encrypting the device data.

- ➔ Initialize the number i.e. num;
  Y = num; sum=0; temp =0;
- ➔ Repeat step until y !=0
  Calculate y%10 and store it in temp
  Calculate temp ^ 3 and add it with the previous value of sum

Update y value with 7/10

- ➔ Check whether the sum is equal to num , if so then Armstrong number otherwise not Armstrong number
- ➔ Assign such Armstrong numbers in database for encrypting the device basic details

Step – 6:

Authenticate the user with the device assigned color combination from the panel selected and allow or disallow the user to access the device for operation.

Step -7:

Once the user authentication is completed, decrypt the device information for user access, using the Armstrong number assigned with device in the database.

Step – 8:

If the user is authenticated for adding the devices, allow to add or allow to update the device details.

Step – 9:

Persist user details along with time stamp at remote location for future references and auditing.

Step – 10 :

If the user fails to detect device in N attempts, User will be automatically detached from the network. Next time, user authentication is valid with color code of the device and also required to provide any security element satisfaction i.e. Date of birth, Aadhaar Card No, PAN Number, Place of birth, etc.

Algorithm implementing environment

The proposed algorithm is implemented in Hadoop platform with SQL Server as backend. The selected platforms support the big data, cloud data, sensor data environments. The details related to the algorithm implementing platforms are follows.

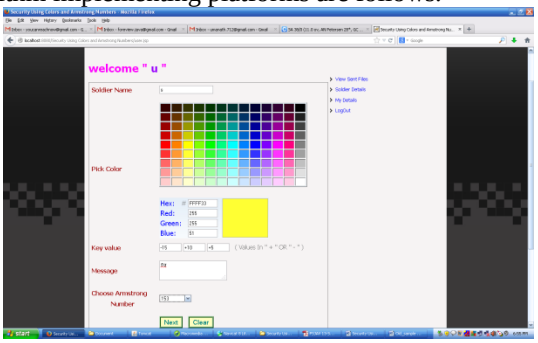


Fig. 1: Color panel for security Authentication and Authorization

Fig. 2: Cryptography implementation Using Armstrong Number

IV Conclusion

The research work done and presented here can be implemented in sensor based devices to connect in the network and access secured way. The encryption methods adopted in this article are efficient and cost effective. As the solution included with optimum utilization of resources and more suitable for reduced space complexity, it can be adopted Big Data, Cloud Data, Wi-Fi networks, and the latest technology environments like Internet of Things (IoT).

It can be a future guide to implement efficient algorithms and solutions to improve performance and security for future coming problems in networking, data security, transferring huge data across different network topologies. The users can also review the architecture mentioned in this thesis and add few components at any internal level and enhance the features for a specific domain. It will be more suitable to face the fore coming complex problems with physical devices, security services, transmission problems, intruders detection.

It will be a guide line for upcoming problems that are beyond the algorithm limit specified. I ensure that it is one of the best references to detect and solve problems related to device management, network management, security management, memory management in any type of applications like different Operating Systems, Mobile systems, Wi-Fi enabled devices and Security systems.

References

[1] M.Karolin1, Dr.T.Meyyapan,"RGB Based Secret Sharing Scheme in Color Visual Cryptography", *International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 7, July 2015*

[2] Pooja and Dr.Lalitha Y. S, "Non Expanded Visual Cryptography for Color Images using Pseudo-Randomized Authentication", in International Journal of Engineering Research and Development, Volume 10, Issue 6 (June 2014)

[3] Manali Naik1, Pushpanjali Tungare2, Pooja Kamble3, Shirish Sabnis4, Color Cryptography using Substitution method, International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056 Volume: 03 Issue: 03- Mar-2016

[4] Kirti Rawat , Vijay Kumar Joshi, Visual Cryptography for Grey Scale Images, International Journal of Computer Science Trends and Technology (IJCST) – Volume 5 Issue 2, Mar – Apr 2017

[5] M PavanKumar, G R RamaDevi, M V Ramana Murthy, A Paradigm to Provide A Secure and Sensitive Ad Hoc Networks, International Journal of Applied Engineering Research (IJAER), Volume 10, Number 1 (2015) *Special Issues*

[6] Gipsa Alex1 , Benitta Varghese2 , Jezna G Jose3 , AlbyMol Abraham4, A Modern Health Care System Using IoT and Android, Gipsa Alex et al. / International Journal on Computer Science and Engineering (IJCSE), 2014.

[7] D.Chitra Devi and V.RhymendUthariaraj," Load Balancing in Cloud Computing Environment Using Improved Weighted Round Robin Algorithm for Nonpreemptive Dependent Tasks", Hindawi Publishing Corporation ,The Scientific World Journal ,Volume 2016, Article ID 3896065, 14 pages.

[8] Kirti Rawat , Vijay Kumar Joshi, Visual Cryptography for Grey Scale Images, International Journal of Computer Science Trends and Technology (IJCST) – Volume 5 Issue 2, Mar – Apr 2017

[9] N Bhaskar, M V Ramanamurthy, Hassan Ismail Mahammud "Security Using Colours & Armstrong Numbers", International Journal of Logistics and Supply Chain Management Perspectives", Pezzottite journals, ISSN: 2319-9032 (Print), 2319-9040 (Online), Volume 6, Number 2 (April to June 2017), pp. 2968-2978. A UGC approved journal No. 45292.

[10] N Bhaskar, M V Ramanamurthy, "Big Data: Data Warehouse and Security", International Journal of Information Technology and Computer Science Perspectives, Pezzottaite Journals, ISSN: 2319-9016 (Print), ISSN: 2319-9024 (Online), Volume 6, Number 1 (January to March, 2017), pp. 2394-2400.

[11] D.ASIR ANTONY GNANA SINGH, E.JEBAMALAR LEAVLINE, "DATA MINING IN NETWORK SECURITY - TECHNIQUES & TOOLS: A RESEARCH PERSPECTIVE", Journal of Theoretical and Applied Information Technology, 20th November 2013. Vol. 57 No.2, ISSN: 1992-8645, E-ISSN: 1817-3195.

[12] Kavita Ahuja, and N.N.Jani, A STUDY OF TRADITIONAL DATA ANALYSIS AND SENSOR DATA ANALYTICS, International Journal of Information Sciences and Techniques (IJIST) Vol.6, No.1/2, March 2016.

[13] Bhavani Thuraisingham, "Secure Sensor Information Management and Mining ", IEEE Signal Processing Magazine, 1053-5888, May 2004.

[14] Dr. Deepti Gupta, Wireless Sensor Networks 'Future trends and Latest Research Challenges', *IOSR-JECE , e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 10, Issue 2, Ver. II (Mar - Apr.2015).*