ISSN: 0975-833X

Availableonlineathttp://www.journalcra.com

International Journal of Current Research
Vol. 11, Issue, 05, pp.3982-3986, May, 2019

DOI: https://doi.org/10.24941/ijcr.35445.05.2019

INTERNATIONAL JOURNAL OFCURRENTRESEARCH

RESEARCH ARTICLE

LIGHT-WEIGHT SECURITY AND DATA PROVENANCE FOR MULTI-HOP INTERNET OF THINGS

***[1]Monica, V., [2]Kalai Selvi, T. and [3]Arun, C.M.**

[1]PG Student, Erode Sengunthar Engineering College, Erode
[2]Assistant Professor, Erode Sengunthar Engineering College, Erode
[3]PG Student, Erode Sengunthar Engineering College, Erode

ARTICLEINFO

Article History:
Received 13th February, 2019
Received in revised form
20th March, 2019
Accepted 18th April, 2019
Published online 30th May, 2019

Key Words:

Light-weight
Multi-hop.

Corresponding author:* **Monica, V.,

ABSTRACT

Due to limited resources and scalability, security protocols for Internet of Things (IoT) need to be light-weighted. The cryptographic solutions are not feasible to apply on small and low-energy devices of IoT because of their energy and space limitations. In this paper, a light-weight protocol to secure the data and achieving data provenance is presented for multi-hop IoT network. The Received Signal Strength Indicator (RSSI) of communicating IoT nodes are used to generate the link fingerprints. The link fingerprints are matched at the server to compute the correlation coefficient. Higher the value of correlation coefficient, higher the percentage of secured data transfer. Lower value gives the detection of adversarial node in between a specific link. Data provenance has also been achieved by comparison of packet header with all the available link fingerprints at the server. The time complexity is computed at the node and server. Level, which is O(1). The energy dissipation is calculated for IoT nodes and overall network. The results show that the energy consumption of the system presented in this paper is 52 mJ to 53 mJ for each IoT node and 313.626 mJ for the entire network. RSSI values are taken in real time from MICAz motes and simulations are performed on MATLAB for adversarial node detection, data provenance and timecomplexity. Experimental results show that up to 97% correlation is achieved when no adversarial node is present in the IoT network.

***Citation: Monica, V., Kalai Selvi, T. and Arun, C.M.,* 2019.** "Light-weight security and data provenance for multi-hop internet of things", *International Journal of Current Research*, 11, (05), 3982-3986.

INTRODUCTION

INTERNET of Things (IoT) comprises a complex network of smart devices, which frequently exchange data through the Internet. IoT has become the necessity for the future communication. It is estimated that 50 billion smart devices will be connected through IoT by 2020. The information of a patient to a medical staff, automobile's performance and statistics, home automation, transportation domain,smart grids and smart meters will be based on IoT. The data acquired from sensors or IoT nodes is propagated to Internet cloud where it is received by the concerned body. The acquired data needs to be accurate and should have the information about its origin. As the number of nodes are large in number, small in size and mostly accessible, the measures should be taken to make sure that the data is secured and efficiently received at the receiving end. Data security and provenance act as backbone in order to implement IoT network because the IoT nodes are not physically protected. The data can easily be forged or tampered if proper security primitives are not taken. Security primitives include detection of certain attacks, masking channel state, intrusion detection, location distinction and data provenance. Provenance is to find the origin of the data. A single change in data might cause big problems e.g., in terms of medical health report generated by an IoT node sent to a doctor, meter reading sent to the company for billing according to the consumption and change in transportation system information. Therefore, the traditional cryptographic techniques are not the viable solution in IoT because of the energy limitations of the IoT nodes. Less space acquiring and energy efficient security primitives with less computational complexities are key building blocks for enabling end-to-end content protection, user authentication, and consumer confidentiality in the IoT world. To ensure the trust of users, the IoT-based network should be secured enough. The security mechanism involved should be light-weighted because of the low energy requirements for IoT nodes. The mutual authentication between IoT nodes with the server should also be secured and authentic. Accurate and secure data provenance in the IoT are used for improving the level of trust. The data provenance is useful for determining and describing the derivation history of data starting from the original resource.

The records can be used to protect intellectual property and its relevance from the perspective of regulatory mechanisms. However, the data provenance integrity is a big question. The data provenance can be forged or tampered by an unauthorized party if the provenance is not properly protected by implementing inefficient security protocols. In order to establish the trust of IoT, a solution to security should be designed which is light-weight and highly secured. Most of the security algorithms and cryptography techniques used today contain high computational complexities with high energy consumption. The solution proposed in this paper incorporates lightweight security algorithms for secured IoT-based information exchange without using extra hardware. Adversarial node is detected effectively by correlating the link fingerprints generated by the adjacent IoT nodes. The correlation coefficient is computed at the server. Data provenance is also achieved using the same link fingerprints generated to find the intrusion detection in the IoT network. Hence, fingerprints are used to authenticate the integrity of data and in the detection of intrusion. The proposed solution has less time complexity compared to other state-of-the-art available solutions. The rapid growth of IoT devices has opened the way for new and exciting applications such as smart cities, smart hospital care, and smart vehicles etc. However, the large amounts of data that these devices may produce and the sensitive nature of this data make the IoT a prime target for cyber attacks. The IoT devices are usually low cost and simple in nature with limited processing, memory, and energy resources. The main security challenges faced by IoT systems include authentication, data integrity, data provenance, privacy, and access control. Moreover, many IoT devices are deployed out in the open and cannot be considered physically secure. Thus, any protocol developed for IoT systems needs to by secure against physical attacks. For example, if an IoT device stores a secret key in its memory, an attacker may launch a physical attack (e.g. optical scrutiny) to read the contents of its memory.

Data provenance establishes trust in the origin and creation process of data. This gives a guarantee that the user can trust the data received from an IoT device i.e., that the data is indeed collected by the specie IoT device at the stated location and time. Self trust or data provenance is critical to the correct operation of the IoT. Recently, several techniques for providing data provenance using hard-ware security primitives have been proposed. Other techniques using the wireless channel characteristics have also been proposed. The authors of propose the use of sensor PUFs to establish data provenance in the IoT. How-ever, if an adversary moves a sensor PUF from its original location the scheme breaks down i.e., the receiver of the data will continue accepting invalid sensor readings without knowing that the location of the data's origin has changed. Similarly, in the authors propose a scheme for data prove-nance using wireless link fingerprints. They use the received signal strength indicator (RSSI) values to generate unique fingerprints. However, their scheme requires the sensor de-vices to store a secret key locally. This requirement exposes their protocol to physical attacks. Moreover, these tech-niques use public key cryptography and have high energy and processing requirements. In this paper we present preliminary work on the devel-opment of a data provenance protocol for IoT systems. The proposed protocol uses PUFs and wireless link fingerprints to ensure self trust and data provenance in IoT systems. The use of a PUF ensures that the user can trust that the data is coming from the stated IoT device. Similarly, the use of wireless link fingerprints ensures that user can trust that the data has been collected from the stated location. Moreover, the proposed protocol does not require IoT devices to store any secret keys which makes it secure against physical at-tacks. The proposed protocol uses PUFs and symmetric key cryptography, making it a light weight and efficient solution for IoT systems.

Literature Survey

1. **Title**: Security in Wireless Sensor Networks: Issues and Challenges

Authors: AhmadSalehi S, M.A. Razzaque, ParisaNaraei, Ali Farrokhtala.

Wireless Sensor Networks (WSNs) are employed in numerous applications in different areas including military, ecology, and health; for example, to control of important information like the personnel position in a building, as a result, WSNs need security. However, several restrictions such as low capability of computation, small memory, limited resources of energy, and the unreliable channels employ communication in using WSNs can cause difficulty in use of security and protection in WSNs. It is very essential to save WSNs from malevolent attacks in unfriendly situations. Such networks require security plan due to various limitations of resources and the prominent characteristics of a wireless sensor network which is a considerable challenge. This article is an extensive review about problems of WSNs security, which examined recently by researchers and a better understanding of future directions for WSN security.

2. **Title**: Biometric-oriented Iris Identification Based on Mathematical Morphology

Authors: Joaquim de Mira Jr. Hugo Vieira Neto. Eduardo B. Neves.

A new method for biometric identification of human irises is proposed in this paper. The method is based on morphological image processing for the identification of unique skeletons of iris structures, which are then used for feature extraction. In this approach, local iris features are represented by the most stable nodes, branches and end- points extracted from the identified skeletons. Assessment of the proposed method was done using subsets of images from the University of Bath Iris Image Database (1000 images) and the CASIA Iris Image Database (500 images). Compelling experimental results demonstrate the viability of using the proposed morphological approach for iris recognition when compared to a state-of-the-art algorithm that uses a global feature extraction approach.

3. **Title**: An effective key management scheme for heterogeneous sensor networks

Authors: Xiaojiang Du, Yang Xiao, Mohsen Guizani, Hsiao-Hwa Chen.

Security is critical for sensor networks used in military, homeland security and other hostile environments. Previous research on sensor network security mainly considers homogeneous sensor networks. Research has shown that homogeneous ad hoc networks have poor performance and scalability. Furthermore, many security schemes designed for homogeneous sensor networks suffer from high communication overhead, computation overhead, and/or high storage requirement. Recently deployed sensor network systems are increasingly following heterogeneous designs. Key management is an essential cryptographic primitive to provide other security operations. In this paper, we present an e□ective key management scheme that takes advantage of the powerful high-end sensors in heterogeneous sensor networks. The performance evaluation and security analysis show that the key management scheme provides better security with low complexity and significant reduction on storage requirement, compared with existing key management schemes.

4. **Title**: Privacy-Preserving Finger code Authentication.

Authors: Mauro Barni, Tiziano Bianchi, Dario Catalano.

We present a privacy preserving protocol for fingerprint based authentication. We consider a scenario where a client equipped with a fingerprint reader is interested into learning if the acquired fingerprint belongs to the database of authorized entities managed by a server. For security, it is required that the client does not learn anything on the database and the server should not get any information about the requested biometry and the outcome of the matching process. The proposed protocol follows a multi-party computation approach and makes extensive use of homomorphic encryption as underlying cryptographic primitive. To keep the protocol complexity as low as possible, a particular representation of ngerprint images, named Finger code, is adopted. Although the previous works on privacy-preserving biometric identification focus on selecting the best matching identity in the database, our main solution is a generic identification protocol and it allows to select and report all the enrolled identities whose distance to the user's finger code is under a given threshold. Variants for simple authentication purposes are provided. Our protocols gain a notable band- width saving (about 8 24%) if compared with the best previous work [1] and its computational complexity is still low and suitable for practical applications. Moreover, even if such protocols are presented in the context of a fingerprint- based system, they can be generalized to any biometric sys- tem that shares the same matching methodology, namely distance computation and thresholding.

5. **Title**: Defending Resource Depletion Attacks on Implantable Medical Devices.

Authors: XialiHei, Xiaojiang Du, JieWu, Fei Hu.

Implantable Medical Devices (IMDs) have been widely used to treat chronic diseases such as cardiac arrhythmia and diabetes. Many IMDs are enabled with wireless communication capabilities and can communicate with an outside programmer/reader wirelessly. With the rapid growth of IMDs, IMD security becomes a critical issue since attacks on IMDs may directly harm the patient. Typical IMDs have very limited resource in terms of energy, computation and storage. In this research, we identify a new kind of attacks on IMDs - Resource Depletion (RD) attacks that could deplete IMD resources (e.g., battery power) quickly. The RD attacks could reduce the lifetime of an IMD from several years to a few weeks. The attacks can be easily launched but cannot be defended by traditional cryptographic approaches. In this paper, we propose to utilize the patient's IMD access pattern and we design a novel Support Vector Machine (SVM) based scheme to address the RD attacks. Our SVM-based scheme is very effective in defending the RD attacks. Our experimental results show that the average detection rate of the SVM-based scheme is above 90%.

6. **Title**: Filter bank-Based Fingerprint Matching

Authors: Anil K. Jain, Fellow, IEEE, Salil Prabhakar, Lin Hong, and Sharath Pankanti

With identity fraud in our society reaching unprecedented proportions and with an increasing emphasis on the emerging automatic personal identification applications, biometrics based verification, especially fingerprint-based identification, is receiving a lot of attention. There are two major shortcomings of the traditional approaches to fingerprint representation. For a considerable fraction of population, the representations based on explicit detection of complete ridge structures in the fingerprint are difficult to extract automatically. The widely used minutiae-based representation does not utilize a significant component of the rich discriminatory information available in the fingerprints. Local ridge structures cannot be completely characterized by minutiae. Further, minutiae-based matching has difficulty in quickly matching two fingerprint images containing different number of unregistered minutiae points. The proposed filter-based algorithm uses a bank of Gabor filters to capture both local and global details in a fingerprint as a compact fixed length Finger Code. The fingerprint matching is based on the Euclidean distance between the two corresponding Finger Codes and hence is extremely fast. We are able to achieve a verification accuracy which is only marginally inferior to the best results of minutiae-based algorithms published in the open literature [1]. Our system performs better than a state-of-the-art minutiae-based system when the performance requirement of the application system does not demand a very low false acceptance rate. Finally, we show that the matching performance can be improved by combining the decisions of the matchers based on complementary (minutiae-based and filter-based) fingerprint information.

7. **Title**: Face Identification by Fitting a 3D Morph able Model Using Linear Shape and Texture Error Functions

Authors: SamiRomdhani, Volker Blanz, and Thomas Vetter
This paper presents a novel algorithm aiming at analysis and identification of faces viewed from different poses and illumination conditions. Face analysis from a single image is performed by recovering the shape and textures parameters of a 3D Morph able Model in an analysis-by-synthesis fashion. The shape parameters are computed from a shape error estimated by optical flow and the texture parameters are obtained from a texture error. The algorithm uses linear equations to recover the shape and texture parameters irrespective of pose and lighting conditions of the face image. Identification experiments are reported on more than 5000 images from the publicly available CMU-PIE database which includes faces viewed from 13 different poses and under 22 different illumina- tions. Extensive identification results are available on our web page for future comparison with novel algorithms.

8. **Title**: A survey of key management schemes in wireless sensor networks

Authors: Yang Xiao, Venkata Krishna Rayi, Bo Sun, Xiaojiang Du.

Wireless sensor networks have many applications, vary in size, and are deployed in a wide variety of areas. They are often deployed in potentially adverse or even hostile environment so that there are concerns on security issues in these networks. Sensor nodes used to form these networks are resource-constrained, which make security applications a challenging problem. Efficient key distribution and management mechanisms are needed besides lightweight ciphers. Many key establishment techniques have been designed to address the tradeoff between limited memory and security, but which scheme is the most effective is still debatable. In this paper, we provide a survey of key management schemes in wireless sensor networks. We notice that no key distribution technique is ideal to all the scenarios where sensor networks are used; therefore the techniques employed must depend upon the requirements of target applications and resources of each individual sensor network.

9. **Title**: Efficient Privacy-Preserving Biometric Identification in Cloud Computing

Authors: Jiawei Yuan, Shucheng Yu

Biometric identification is a reliable and convenient way of identifying individuals. The widespread adoption of biometric identification requires solid privacy protection against possible misuse, loss, or theft of biometric data. Existing techniques for privacy-preserving biometric identification primarily rely on conventional cryptographic primitives such as homomorphic encryption and oblivious transfer, which inevitably introduce tremendous cost to the system and are not applicable to practical large-scale applications. In this paper, we propose a novel privacy-preserving biometric identification scheme which achieves efficiency by exploiting the power of cloud computing. In our proposed scheme, the biometric database is encrypted and outsourced to the cloud servers. To perform a biometric identification, the database owner generates a credential for the candidate biometric trait and submits it to the cloud. The cloud servers perform identification over the encrypted database using the credential and return the result to the owner. During the identification, cloud learns nothing about the original private biometric data. Because the identification operations are securely outsourced to the cloud, the real time computational/communication costs at the owner side are minimal. Thorough analysis shows that our proposed scheme is secure and offers a higher level of privacy protection than related solutions such as kNN search in encrypted databases. Real experiments on Amazon cloud, over databases of different sizes, show that our computational/communication costs at the owner side are several magnitudes lower than the existing biometric identification schemes.

10. **Title**: Security Analysis of Collusion-Resistant Nearest Neighbor Query Scheme on Encrypted Cloud Data

Authors: Youwen ZHU, Tsuyoshi TAKAGI, Rong HU.

Recently. Yuan ET at (IEEE lnfocom '13. pp.2652-2660) proposed an efficient secure nearest neighbor (SNN) search scheme on encrypted cloud database. Their scheme is claimed to be secure against the collusion attack of query clients and cloud server. Because the colluding attackers cannot infer the encryption/decryption key.In this letter. We observe that the encrypted dataset in Yuan's scheme can be broken by the collusion attack without deducing the key, and present a simple but powerful attack to their scheme. Experiment results validate the high efficiency of our attacking approach. Additionally. We also indicate an upper bound of collusion-resistant ability of any accurate SNN query scheme.

Objective of The Project

- To provide security in lightweight manner resource mobile devices in cloud environment
- To have light weight revocation policy. The encrypted and decrypted data should be secure using secret key.
- The sharing of the file should be among the authorized users who have the access privileges.

There should also have the opportunity to decrease the overhead of the cryptographic standard algorithm and research the security schemes with low overhead.

Existing System

The numbers of nodes are large in number, small in size and mostly accessible, the measures should be taken to make sure that the data is secured and efficiently received at the receiving end. Data security and provenance act as backbone in order to implement IoT network because the IoT nodes are not physically protected easily be forged or tampered if proper security primitives are not taken. Security primitives include detection of certain attacks, masking channel state, intrusion detection, location distinction and data provenance. Provenance is to find the origin of the data. A single change in data might cause big problems e.g., in terms of medical health report generated by an IoT node sent to a doctor, meter reading sent to the company for billing according to the consumption and change in transportation system information. Therefore, the traditional cryptographic techniques are not the viable solution in IoT because of the energy limitations of the IoT nodes.

Drawbacks of Existing System

Less space acquiring and energy efficient security: Primitives with less computational complexities are key building blocks for enabling end-to-end content protection, user authentication, and consumer confidentiality in the IoT world.

Proposed System

The proposed trust model is described for cloud computing in. High trust can be achieved using the same model in IoT environment. Improved energy efficiency is achieved by using Gale-Shapley algorithm which matches D2D pair with cellular user equipments (UEs). Correlation among UEs are analyzed using a game-theoretic approach. Lightweight security algorithms for secured IoT-based information exchange without using extra hardware. Adversarial node is detected effectively by correlating the link fingerprints generated by the adjacent IoT nodes. The correlation coefficient is computed at the server. Data provenance is also achieved using the same link fingerprints generated to find the intrusion detection in the IoT network. Hence, fingerprints are used to authenticate the integrity of data and in the detection of intrusion. The proposed solution has less time complexity compared to other state-of-the-art available solutions.

Advantages

1). No adversarial node is present in the IoT network
2) Adversarial node is present in between two communicating IoT nodes
3) The packet is forged or tempered at any IoT node
4) The IoT node is replaced by adversarial node
5) The server is not secured in a way that adversarial node can send its data to the server but cannot access the data present at the server
6) Finding the intrusion in later data using provenance Algorithm.

Modules

- Register
- Login
- Upload & Search Products
- View Users & Key request
- View Nodes products & Purchase History

Register

- The registration module allow the user to create login username and the password by submitting their information like mail id, phone number, name, etc.
- By registering the network or cloud the user can gain access to the resources stored in the cloud.

Login

- In this module the user can login by using their unique username and password.
- The login module verify the user given username and password with the stored username and password in the cloud.
- If the username and password is matched the user can access the resources.
- If it does not match the user does not allowed to access the resource.

Upload & Search Products

- The node users can add the product to the server.
- The node users can view the product by searching.

View users & Key Request

- The IOT server can view all the IOT Nodes.
- And also manage the key request from the Iot Nodes.

View nodes products & purchase history

- The Iot Servers can view all the products that was uploaded by the Iot Nodes.
- And also can view the Purchase history of the Iot Nodes.

Conclusion

This paper presents preliminary work for a data prove-nance technique for the IoT using PUFs and wireless link ngerprints. The spatio-temporal characteristics of a wire-less channel are exploited to generate the wireless link nger-prints. By combining wireless link ngerprints with PUFs, the proposed protocol achieves security against physical at-tacks. Moreover, the protocol achieves its desired security goals e ciently using symmetric key encryption. The pro-posed protocol uses RSSI values to generate the wireless link ngerprints. A preliminary security and performance analy-sis show that the proposed protocol can achieve the desired security goals e ciently. However, a more detailed and ex-perimental evaluation of the proposed protocol is required to evaluate the performance and security of the proposed protocol.

Future Enhancement: Concerning illustration for late, various investigations with respect to get to control in the cloud rely on upon property based encryption count (ABE). To At whatever case, traditional ABE isn't proper to the versant cloud since it may be computationally escalated Furthermore cell phones recently has confined benefits. In this paper, we recommend LDSS address this issue. It displays An novel LDSS-CP-ABE computation on move true figuring overhead starting with Mobile phones onto go-between servers, in this way it might fare thee well of the ensured data imparting issue in the versant cloud Later on work, we will framework better approaches should manage assurance data respectability. Should Moreover tap the proficiency about the convenient cloud, we will similarly inspect how with do ciphertext recuperation through existing data imparting arrangements.

REFERENCES

Ali, S. T. et al., \Securing Data Provenance in Body Area Networks using Lightweight Wireless Link Fingerprints," Proc. TrustED, November 2013.

Aman M. N. et al., \Physical Unclonable Functions for IoT Security," Proceedings of ACM AsiaCCSIoTPTS, June 2016.

Bertino, E. \Data Security and Privacy in the IoT," Proc. EDBT, March 2016.

Bohm, C. and M. Hofer, \Physical Unclonable Functions in Theory and Practice," Springer, 2012.

Cheng, D. *et al.,* \Wireless Device Authentication Using Acoustic Hardware Fingerprints," Proc. Int. Conf. on Big Data Computing and Communications, 2015.

Jakes. W. C. \Microwave Mobile Communications". Wiley, 1974.

Kanuparthi A. et al., \Hardware and Embedded Security in the Context of Internet of Things," Proc. ACM CyCAR, November 2013.

Maes, R. Physically Unclonable Functions: Constructions, Properties and Applications," Katholieke Universiteit Leuven Belgium DEngg Thesis, 2013.

Rasmussen K. B. and S. Capkun.\Implications of Radio Fingerprinting on the Security of Sensor Networks," Proceedings of Secure Comm, September 2012.

****