Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 65 Issue 07 | 2022
DOI 10.17605/OSF.IO/4BA7F

A TRUST BASED DATA SECURITY MODEL FOR WIRELESS SENSOR NETWORKS COMMUNICATION

SUMAN DEVI[1] and AVADHESH KUMAR[2]

[1]PhD Scholar, School of Computing Science & Engineering, Galgotias University, India.
E-mail: Suman14vashisth@gmail.com
[2]Professor, School of Computing Science & Engineering, Galgotias University, India.
E-mail: avadheshkumar@galgotiasuniversity.edu.in

Abstract

A large amount of data is produced in this modern age. Due to the open and connected world, the data and its privacy is always at risk. As a result, enabling data exchange for real large data in cyberspace is extremely tough. We propose an architecture that offers a safe and authentic data exchange algorithm in this modern and connected world. The proposed approach will provide better security in present day cyberspace. The paper presents a trust based Wireless Sensor Network (WSN) system with secure data sharing; Design an intelligent security model to enhance WSN security; A trusted value-exchange method for purchasing security services, which allows users to earn financial benefits for contributing their data or services, hence encouraging data sharing. Furthermore, we examine our performance for network security and economic income, as well as its potential alternate deployment methods. The output is compared in terms of randomness, hardness and successful key reconciliation. The proposed model offers a more secure and authentic security framework for large datasets.

Keywords - Cyberspace, Data Sharing, Wireless Sensors, Security, Trust Model

1. INTRODUCTION

Data is the owner's asset in social, cyber, and physical (SCP) systems and its usage should be under his or her total control, however this is not often the case [1]. That is, an individual's inability to effectively handle data makes controlling the possible hazards linked with the obtained data extremely difficult [9]. Meanwhile, the lack of permanent records for data consumption raises the danger of misuse [10]. A trust based WSN Model is shown in Figure 1.

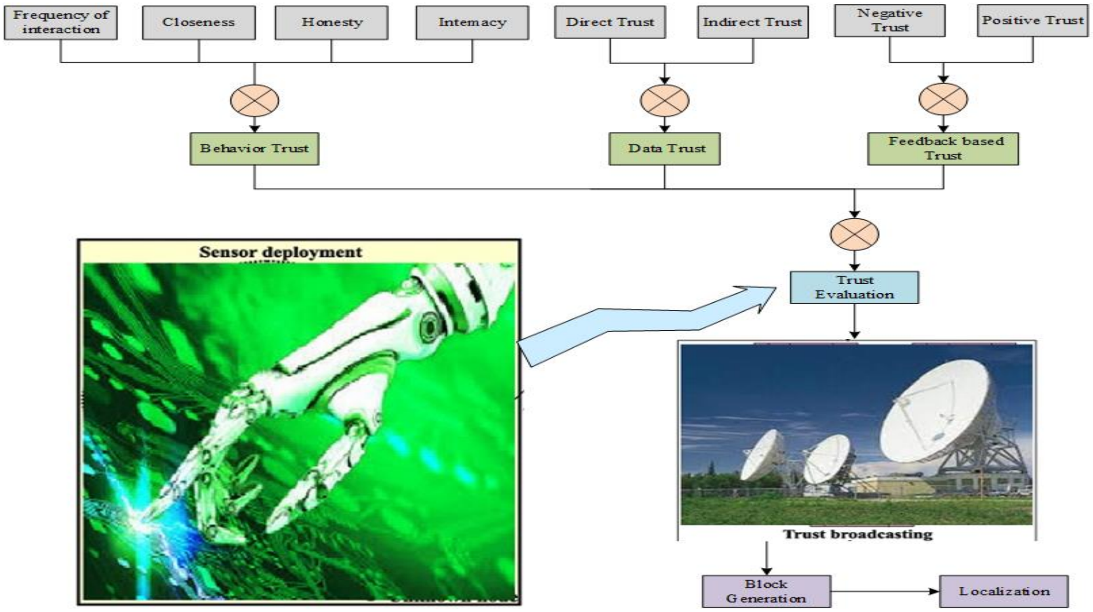

Fig 1: A trust based WSN model.

Because AI algorithms demand a large quantity of data from as many places on the Internet as feasible, data security is one of the most important problems for any network design. Amber architecture for detaching data from online programs presented [3]. The open PDS is a safe virtual environment where users may collect their data, while preventing any program from directly accessing the data. It was created by a team of researchers at MIT's Media Lab [5]. The Origin Chain system was created by the developers of [8] to realize the metadata's transparency and tamper-proof properties. All parties engaged in the Origin Chain may access the same accurate data and adapt to changing conditions and requests. In [10], the authors suggest a WSN-based MeD Share system the work in [14] provides a detailed analysis of WSN and Intrusion Detection System (IDS) history, examines how to integrate WSN technology to IDS, and makes educated judgments about potential hidden risks in this approach. AI is a viable technique to improve data security in CPS because it can analyze large amounts of data in depth, identify hidden patterns, and then make correct predictions, thanks to the availability of large amounts of data and improved computing power [15]. [11] Provides a comprehensive review of potential future research areas, such as how to increase data security with AI. Illustrates how AI can perform better if given a vast quantity of data to construct a better base model, and calls for additional efforts to be made to produce greater useful datasets to empower AI for improved data security.

There are a large number of security algorithms proposed over the years. All the security algorithms studies thus far are heavy and complex. We aim to build a security framework that will be useful in real time systems. This would have significant advantages (for example, improved data security) and might possibly allow AI to surpass human skills in other domains [13]. Fortunately, WSN technologies may be a promising solution to achieve this aim. As a result, WSN-protected data exchange can help AI become even more powerful [14]. As a result, improved AI has the potential to improve data performance and security. Furthermore, the study in [10] provides an overview of AI approaches for cyber security and includes a detailed review. Furthermore, the work in [12] intends to create a market where people may trade security modes for greater data protection. However, none of them looks at data security from an architectural standpoint. To close this gap, proposed algorithm aims to build a novel security and authentication mechanism to provide improved security to large datasets. Author's contribution to the paper is as follows

In this study, we propose novel trust-based security mechanisms for WSN technology and data. We set up new Integrity checkpoints to enhance security of WSN SCP data.

- A secure platform is established for large datasets WSN Technology. The proposed algorithm dramatically increases data sharing security, as well as the security of the entire network, including the whole SCP.
- One of the most major difficulties in proposed algorithm is determining where to keep data [1]. This is due to the stymies of data security and application innovation. Proposed algorithm inherits and uses PDR (Private Data Reservoir) instead of PDSR (Personal data store repository) [5].

Each PDR acts as a safe and centralized physical location for each proposed algorithm user's data. By incorporating PDR into Proposed algorithm, users will have complete control over their data and accomplish fine-grained monitoring of data access behaviors. Actually, in addition to PDR, various options for data storage in proposed algorithm can be used depending on the requirements. Because of the lack of trust between different data stakeholders, data sharing across the Internet is severely constrained, and the data utilized for AI training and analysis is both restricted in quantity and incomplete in diversity. Fortunately, the emergence of WSN technology has brought with it an optimistic and efficient that can aid AI in making more correct judgments by utilizing actual large data collected from more locations on the Internet. Proposed algorithm makes use of developing WSN technology to avoid data misuse.

2. LITERATURE REVIEW

Because AI algorithms demand a large quantity of data from as many places on the Internet as feasible, data security is one of the most important problems for any network design. Meanwhile, a more powerful AI can defend data security at a higher level, since an upgraded AI can figure out complex and intricate threats more quickly than a standard AI. A variety of measures are being made to improve data security in the CPS. The work in [3] proposes Amber architecture for detaching data from online apps, which offers web users control over their personal data and provides a strong web-wide query mechanism for searching personal data. The open PDS [5] is a secured virtual space for users to collect, store, and manage their data, separating all kinds of applications from operating on data directly. It was designed by a research group from the Media Lab at Massachusetts Institute of Technology to extend the decoupling mechanism of data and applications from only web services to all kinds of applications. Furthermore, open PDS presents Safe Answer, a new service paradigm for dynamically protecting data privacy by decreasing the dimensions of personal data.

Furthermore, by providing tamper-proof and traceable recording features as well as incentive mechanisms, the new block chain technology offers an efficient and effective solution to ensure the security of data in CPS. When the supply chain traces products, the authors of [8] create the Origin Chain system to actualize the metadata's transparency and tamper-proof characteristics. Origin Chain allows all parties involved to access the same reliable data and react to changing circumstances and requirements. In [10], the authors suggest a block chain- based MeD Share system for successfully managing and protecting medical records, as well as sharing medical data among cloud repositories, with assurances on data provenance, auditing, and control. The work provides a detailed analysis of block chain and Intrusion Detection System (IDS) history, examines how to integrate block chain technology to IDS, and makes educated judgments about potential hidden risks in this approach. Furthermore, the work in [15] proposes a block chain-based incentive structure for crowd sensing applications that preserves anonymity while ensuring data security. Furthermore, AI is a viable technique to improve data security in CPS because it can analyze large amounts of data in depth, identify hidden patterns, and then make correct predictions, thanks to the availability of large amounts of data and improved computing power. [11] Provides a comprehensive review of the use of AI for big data as well as the use of big data for AI, as well as potential future research areas, such as how to increase data security with AI. Illustrates how AI can perform better if given a vast quantity of data to construct a better base model, and calls for additional efforts to be made to produce greater useful datasets to empower AI for improved data security. Furthermore, the study in [12] provides an overview of AI approaches for cyber security and includes a detailed review. Furthermore, the work in [14] intends to create a market where people may trade machine learning modes for incentives, making AI more realistic and accessible to everyone and, as a result, delivering more AI solutions for greater data protection. However, none of them looks at data security from an architectural standpoint. To close this gap, proposed algorithm aims to build a common and general networking architecture by combining the power of AI and block chain on a large scale, which can support dynamic updates of all these functional components individually at any time as needed, thereby improving data security for all applications efficiently and effectively.

3. NETWORK MODEL

In the Internet of Things, data is interpreted by nodes that work with one another. The three categories of IoT nodes that may be categorized based on their responsibilities are base station (BS), cluster head (CH), and sensor nodes. This research offers IoT network architecture to make managing these nodes and implementing secure authentication amongst them easier. Before accessing or interacting with a node's data as a client, the end user must be validated in order to obtain authorization. End users are frequently provided with appropriate processing. Identity identification is one of the most important ways for guaranteeing IoT security.

Proposed algorithm is a network design that integrates three critical components to create a more secure cyberspace: 1) A trust based WSN system with secure data sharing; 2) Designing am AI based intelligent security rules to enhance WSN security; 3) A trusted value-exchange method for purchasing security services, which allows users to earn financial benefits for contributing their data or services, hence encouraging data sharing and improving AI performance.

• Setting up the system. It relies heavily on the BS to set the security settings.

• Registration. Each node's identification information is recorded and saved on the public WSN at this step.

• Stage of authentication. The hybrid WSN approach suggested above validates and authorises various sorts of authentication requests at this step; node logout In the event of damage, assault, or energy exhaustion, the node must be logged out.

3.1 Initialization

All nodes in the subnet must be initialized before the base station may deploy nodes. To begin, the base station determines each node's identity, including its own. The bases station obtains the node's unique identification IDi = hash (EAi) and transmits it to each node for storage using the hashing algorithm. Ordinary ID (OID) is used to identify ordinary nodes, Cluster ID(CID) is used to identify cluster head nodes, and Station ID is used to identify base stations (SID). The base station then creates a set of public-private key pairs for each node, known as publickeyu / privatekeyu (puku/prku). They are not repeated in the following descriptions because the procedure is identical. Finally, each node requires an ID card from the base station to establish its unique identification.

3.2 Registration

The objective of node deployment is to build a complete network topology by equally distributing nodes throughout the network.

3.2.1 Registration of cluster node

Registration transaction request messages are submitted by the cluster head nodes. Registration is needed (EACID, CID, EASID, SID, ID card CID). Then, on the public WSN, activate the smart contract that will carry out the registration verification procedure, and complete the stages in order:

1. Query the node identification information contained in the public WSN to see if cluster head nodes already exist, and if they do, fail to validate.

2. Using the Ethernet address composition structure, check the authenticity of the EACID.

3. Verify the validity of the CH ID card CID.

When all of the procedures are properly confirmed, the public WSN saves the cluster head node's identification information in the manner described above and publishes the message that has been validated. CH is given permission to access the network via the local WSN.

3.2.2 Registration of simple node

The registration procedure is completed in the following order:

The smart contract's local WSN node receives all nodes' identity information.

1. Check the base station's SID for authenticity.
2. Check the cluster head node's CID for authenticity.
3. Verify that the cluster head node identity nameplate IDcardOID is accurate. Registration as well as the base station’s public key is required.

3.3. Authentication for simple nodes.

When node A starts the authentication process, it sends the Request of Connection (AOID, ACID, ASID, BOID, IdcardA) message to the CH node.

1. Check the AOID and BOID nodes' states; if neither is alive, return an error.
2. Move to step (5) if nodes A and B are on the same WSN subnet; otherwise, go to step 6. (6).
3. The identification information of nodes A and B is queried by the local WSN based on the node identity information contained in the WSN.
4. According to the node identification information contained in the WSN, the public WSN queries the identity and delivers confirmation messages. After verification, send a message of confirmation to CH. The public WSN transaction voucher is Voucher of Transaction=keccak (AOID, BOID, local block. timestamp). Cluster head node ASID transmits the signed result SignedA (Credential of Authentication A).

4. RESULT AND ANALYSIS

In this part, we discuss the security needs for IoT devices and provide an analysis. In most cases, integrity refers to both data and message integrity. Unauthorized users and devices cannot access or alter data stored in the IoT, which is referred to as data integrity. This is the goal of the authentication technique presented in this work. Message integrity means that during the interaction process, the messages sent by users and IoT devices cannot be tampered with unlawfully. In this article, the authentication procedure is carried out on both the public and local WSNs. Each transaction is verified for integrity and cannot be tampered with once it has been submitted. The authentication mechanism ensures the message's integrity.

The term "availability" refers to the ability of genuine users and devices to utilize the IoT's services. Denial of service attacks must be avoided at all costs. Later, we'll look at denial of service threats in the context of identity authentication.

For IoT, scalability is a critical security need. Because of the features of IoT equipment, it is often replaced. Scalability emerges as the primary way of resolving this issue. The authentication system presented in this article effectively authenticates genuine nodes, allows access to the network, and revokes access to invalid nodes while also meeting scalability criteria.

The identities of the two transmitters must be acknowledged before they communicate, which is known as mutual authentication. The authentication system described in this study identifies the authenticated party via the ordinary node's direct management node. To satisfy the following security needs, authentication techniques are needed to withstand some of the most prevalent network assaults in the IoT.

The authentication process' complex calculations and large storage requirements are handled BS. The output of the proposed approach is measured in terms of successful key reconciliation rate. The successful key reconciliation rate is shown in Fig. 2.

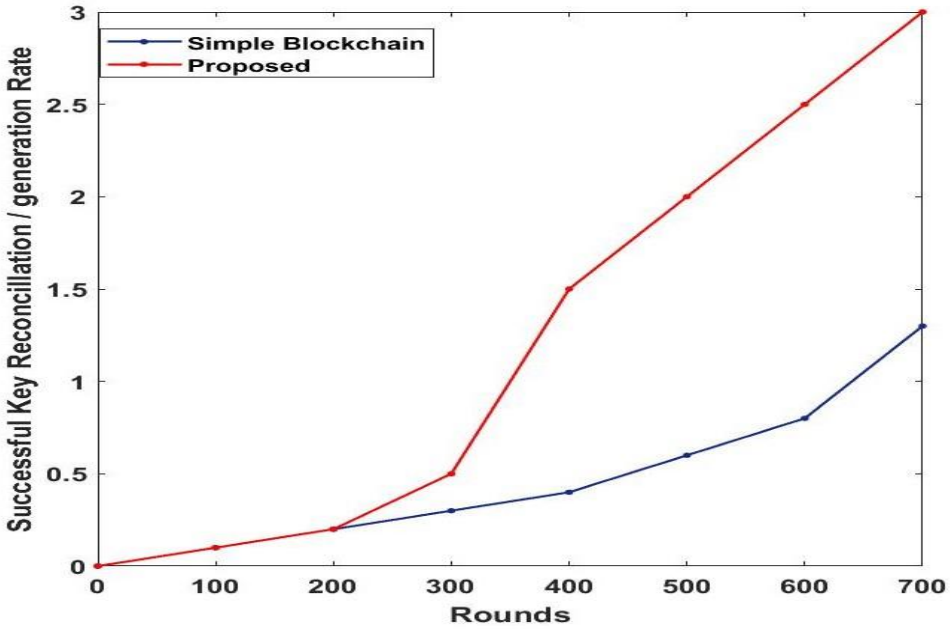

Fig 2: Key success rate.

Hardness measures the effectiveness of the security algorithm. Proposed approach emphasis of harness to make it more secure against outside attacks. Harder is the security framework, more difficult it is to break. The proposed approach secure data and information based on authentication keys whose harness is ensured by key randomness. The proposed algorithm is measured in terms of hardness. The hardness output is shown in Fig. 3. It is seen that the hardness increases with increase in rounds.

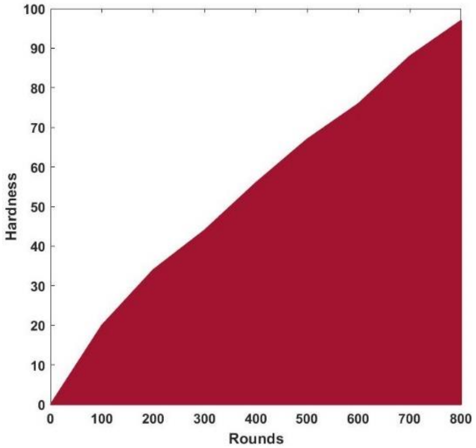

Fig 3: Hardness of the proposed approach.

The majority of node energy consumption in the IoT is used for message transmission. In this section, the size of messages sent by nodes serves as the benchmark for comparison. In terms of processing, storage, and energy consumption, the system in this article is in line with the design assumptions, and it has a very high performance, as assessed by three parts of analysis. Figure 4 depicts the suggested approach's network energy usage.

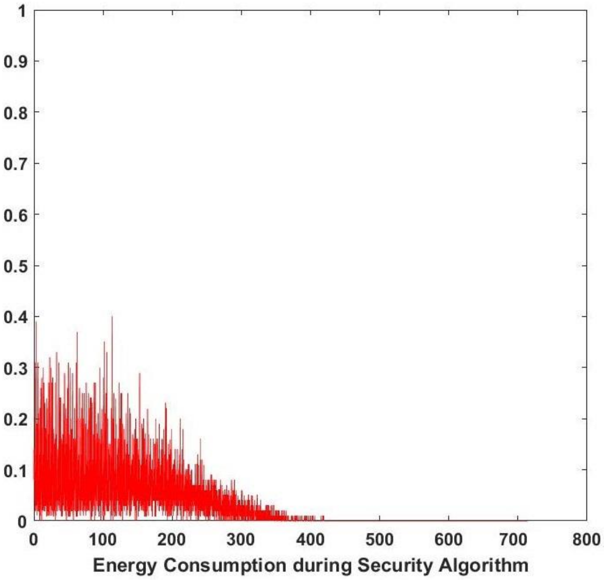

Fig 4: Network Energy consumption of the proposed approach.

The proposed approach's output is also measured in terms of key randomness. More is the randomness of the security algorithm; harder it is to break. The proposed approach introduces an increased randomness in the encryption keys, increasing the security and hardness of the algorithm. The randomness is shown by Fig. 5 which shows the efficiency of the proposed approach. It is seen from Fig. 5 that the key randomness increases with increase in rounds.

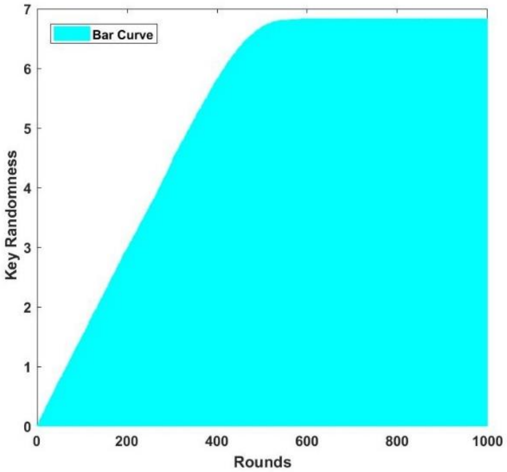

Fig 5: Key randomness increase with rounds.

5. CONCLUSION

This article offers a multi-WSN identity strategy based on WSN to address the single point failure of existing authentication methods in IoT. A private WSN is built between CH and BS, combining the decentralization of WSN. The whole network is built on a hybrid WSN paradigm. The registration of identification information, as well as communication authentication between nodes, is accomplished in this architecture. Finally, the scheme's security and efficiency are demonstrated by the security and performance study. This work can be expanded in future by including more IoT performance parameters such as latency and throughput.

References

1. H. Yin, D. Guo, K. Wang, Z. Jiang, Y. Lyu, and J. Xing, ''Hyper connected network: A decentralized trusted computing and networking paradigm,'' IEEE Netw., vol. 32, no. 1, pp. 112–117, Jan./Feb. 2018.
2. K. Fan, W. Jiang, H. Li, and Y. Yang, ''Lightweight RFID protocol for medical privacy protection in IoT,'' IEEE Trans Ind. Inform at., vol. 14, no. 4, pp. 1656–1665, Apr. 2018.
3. T. Chajed, J. Gjengset, J. Van Den Hooff, M. F. Kaashoek, J. Mickens, R. Morris, and N. Zeldovich, ''Amber: Decoupling user data from Web applications,'' in Proc. 15th Workshop Hot Topics Oper. Syst. (HotOS XV), Warth-Weiningen, Switzerland, 2015, pp. 1–6.
4. M. Lecuyer, R. Spahn, R. Geambasu, T.-K. Huang, and S. Sen, ''Enhancing selectivity in big data,'' IEEE Security Privacy, vol. 16, no. 1, pp. 34–42, Jan./Feb. 2018.

5. Y.-A. de Montjoye, E. Shmueli, S. S. Wang, and A. S. Pentland, ‘‘open PDS: Protecting the privacy of metadata through Safe Answers,’’ PLoS ONE, vol. 9, no. 7, 2014, Art. no. e98790.
6. C. Perera, R. Ranjan, and L. Wang, ‘‘End-to-end privacy for open big data markets,’’ IEEE Cloud Comput., vol. 2, no. 4, pp. 44–53, Apr. 2015.
7. X. Zheng, Z. Cai, and Y. Li, ‘‘Data linkage in smart Internet of Things systems: A consideration from a privacy perspective,’’ IEEE Commun. Mag., vol. 56, no. 9, pp. 55–61, Sep. 2018.
8. Q. Lu and X. Xu, ‘‘Adaptable WSN-based systems: A case study for product traceability,’’ IEEE Softw., vol. 34, no. 6, pp. 21–27, Nov./Dec. 2017.
9. Y. Liang, Z. Cai, J. Yu, Q. Han, and Y. Li, ‘‘Deep learning based inference of private information using embedded sensors in smart devices’’ IEEE Netw. Mag., vol. 32, no. 4, pp. 8–14, Jul. /Aug. 2018.
10. Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, ‘‘MeD Share: Trust-less medical data sharing among cloud service providers via WSN,’’ IEEE Access, vol. 5, pp. 14757–14767, 2017.
11. D. E. O'Leary, ‘‘Artificial intelligence and big data,’’ IEEE Intell. Syst., vol. 28, no. 2, pp. 96–99, Mar. 2013.
12. A.Halevy, P. Norvig, and F. Pereira, ‘‘the unreasonable effectiveness of data,’’ IEEE Intell. Syst., vol. 24, no. 2, pp. 8–12, Mar. 2009.
13. Z. Cai and X. Zheng, ‘‘A private and efficient mechanism for data uploading in smart cyber-physical systems,’’ IEEE Trans. Netw. Sci. Eng., to be published. doi: 10.1109/TNSE.2018.2830307.
14. A.Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, ‘‘WSN: A distributed solution to automotive security and privacy,’’ IEEE Commun. Mag., vol. 55, no. 12, pp. 119–125, Dec. 2017.
15. J. Wang, M. Li, Y. He, H. Li, K. Xiao, and C. Wang, ‘‘A block chain based privacy-preserving incentive mechanism in crowd sensing applications,’’ IEEE Access, vol. 6, pp. 17545–17556, 2018.