A Hardy Wall Encrypted System for Securing IoT Device Id

M. Sundarrajan, A.E. Narayanan

Abstract: Internet of Things (IoT) is being used immensely in numerous areas to reduce human and machine interactions. In an IoT environment, all the devices are connected to one another via the internet to communicate and work for a specific task. When it comes to IoT security, it still needs ample development as data leaks and security breaches still occur. Various research works have focused on securing the data being transmitted through various devices but have shown minimal focus on securing the device itself. In this research work, we propose a model exclusively built for an IoT environment namely "Hardy Security System" that works on securing the Device ID instead of securing the data being transmitted from the devices. The proposed system makes use of Fermat's theorem and various steps involved in building this system is widely discussed in this paper. Use of advanced mathematical cryptology is rigorously done to minimize the security threats in the system. Various performance metrics are concerned and the overall performance analysis is observed to be more efficient than the traditional systems. The proposed system has reduced the overall data leak up to 20%from 80%. With the use of Hardy Wall algorithm the communication bandwidth saw a decrease from 5% to 3%. NS3 proved to be more efficient for performing and evaluating the results by making use of minimal memory consumption. The use of fake IDs were limited by about 2% and the factor of communication bandwidth was also considered. This makes the system safer for communication by reducing the risk of hacking the systems.

Keywords: *IoT, Security, Fermat's Theorem, Cryptography, Communication, Hardy Wall*

I. INTRODUCTION

IoT has gained seamlessly efficient popularity in the era of technological development. IoT is an interconnection of numerous computing devices in an internet-based environment. We tend to use numerous computing devices in our daily life such as our smartphones, cars, home appliances, electronic gadgets, and the list goes on [1]. IoT is a technology that connects all the devices and makes controlling of these devices in a very efficient manner by centralizing it. IoT is extensively used in many fields some of them being automobiles [2], industrial appliances [3], healthcare [4], smart homes [5] and even in entertainment [6]. Use of IoT has eased many everyday activities and has also made many changes in the way by which people interact with each other and also with other computing devices. It is well known that the total amount of people present on the planet is very minimal when compared to the total number of devices connected to the internet. This arises a situation where a massive amount of data are sent and received through these devices. A lot of information is also stored in these devices which makes it vulnerable to intense security breaches and gives rise to many new hackers. This paves the way for a need for efficient and secured IoT systems [7]. A lot of researchers are working on securing the IoT environment and numerous researches have been successful too. Even small applications such as Smart cards, Access cards, and bus cards needs to be secured from data breaching. All the IoT based devices consist of personal and private information about the user of the device. Though IoT eases numerous work of everyday activity, it does not guarantee the security of our data. A small leak in the signal of communication happening between two connected devices in an IoT environment can cause severe damage to the entire IoT environment. Though many security systems are being built to make the communication secure, there are various other ways in which the hackers are able to break the system and steal the information. Hence, the security of an IoT environment can never become an obsolete area of research as tomorrow's entire communication would take place only through these interconnected smart devices.

Most of the related works on IoT security largely deals with securing the communication that happens between the devices. In this paper, we have concentrated on securing the device that takes place in the communication rather than securing the data being transmitted in the communication process. The security of the device is guaranteed by providing a secure IDOT (Identity of Things). All the devices taking part in the communication has its own unique device ID. The system proposed in the paper concerns on securing this Device ID. An efficient Hardy Wall Algorithm is designed for the system used Fermat's Theorem and mathematical cryptography. The system is compared with the existing systems and is observed to perform better than the traditional systems. The rest of the section is as follows: Section II consists of related works, Section III consists of the algorithm and various methods used in securing the device ID. Section IV consists of various experimental results obtained and the performance evaluation. The paper is concluded in the last by mentioning the relevant future works that could be applied or added to the proposed work.

Revised Manuscript Received on 30 May 2019.

***** Correspondence Author
M.Sundarrajan*, Computer Science and Engineering, Periyar Maniammai Institute of Science & Technology, Thanjavur, India.
A.E.Narayanan, Computer Science and Engineering, Periyar Maniammai Institute of Science & Technology, Thanjavur, India.

II. RELATED WORK

IoT is an environment where numerous devices are connected where each device has its own unique device ID. In this paper, we have proposed a method where the computing devices taking part in the communication is secured. There are numerous applications where IoT is being used and it needs to be secured for not misusing the information being transmitted within the environment. FK Santoso [8] has made use of asymmetric elliptical curve cryptography for authentication purposes and built a smart home framework. An IoT network architecture is built and discussed in [9] where all the security challenges prevailing in an IoT environment are analyzed. An efficient algorithm named " EAMSuS" is also built for Smart City framework. The algorithm secures the surveillance system of an entire city. IoT is vigorously used even in agricultural fields. An information management scheme is proposed by Ji-Chun Zao that collects data required for the agricultural research facilities. The system consists of remote sensing along with internet and wireless communication that adds an advantage to the proposed system [10].

Many researchers have previously worked on securing the information that is being transmitted within the IoT environment. Van Kranenburg [11] has discussed the various challenges faced by the IoT environment. The research work gives us a gist about the various areas that need to improvise to make an IoT environment secured. In [12], the IoT frameworks used in securing the entire communication between the IoT devices are discussed. In [13], various Intrusion Detection schemes are surveyed that play a vital role in detecting various attacks in an IoT based environment. Wireless Sensor Networks(WSNs) play a vital role in communicating within an industrial IoT environment. These WSNs were initially secured by using a two-way authentication technique proposed by Jiang et al. [14]. Mikolaj [15] has introduced an advanced technique of factorizing multi-bit numbers which is completely based on Fermat's theorem. Fermat's theorem is commonly used for all the algorithms that involve applications based on factorization [16].

Password acts as one of the most important authentication processes where only the authorized user can get access to the data being transmitted within the IoT environment. Though the password is issued for securing the environment, there are numerous loopholes, that break the security of the communication gets access to the environment. In [17], a password authentication protocol is specially designed for heterogeneous wireless sensor networks. Filippo Gandino increased the overall security level by integrating a new routine with a well-known key computation mechanism purely based on the transitory master secret [18]. The experimental analysis claimed that the proposed routine reduced the computational time while increasing the overall security. In [19], secure communication is proposed by making use of cryptographic key distribution. It also made use of randomized distributed algorithms and proposed a shared key discovery where an only minimal amount of information is broadcasted through the entire channel. Xiong Li et al. has reviewed a two-factor authentication scheme proposed by Jiang et al. [20] where the security flaws were identified. In order to overcome the identified flaws, a three-factor anonymous authentication scheme is been proposed for WSNs in an IoT environment. The results are compared and are claimed that the proposed approach has increased the computational efficiency and has achieved better security when compared to the previous approaches [21].

III. MATHEMATICAL FORMULATION AND DISCUSSION

IDoT is a Unique Identifier (UID) that is assigned to each and every device and things connected with the internet in an IoT environment. The UID plays a vital role in communicating between the devices and exchanging the information to do a particular task. It is claimed by Gartner [] that 25% of security attacks in a network occurs due to poor and insecure device IDs and could be minimized to about 10% when the device ID is just protected toughly by verbalizing encryption. In this paper, we have proposed a model that is designed to effectively secure these vulnerable device Ids and minimize the number of security attacks in the network. This section discusses the proposed system model and Hardy Wall algorithm that has been proposed in this work.

System Model

The system consists of an IoT environment where numerous applications are present and various services are offered to any particular user of the system. There are various uses and devices that are connected to this environment to make use of the applications provided. Each user has a unique user ID and each device has it unique device Ids and they might be from any location. These IDs are the unique identities of the users and the devices. The messages communicated within this system and between various devices are transmitted only through these unique identities. In our work, we have proposed a Hardy Wall Algorithm between the IoT environment and the devices for secure transmission of messages and to prevent data leaks. The overall system model is depicted in Fig.1. The Hardy Wall Algorithm that is used for securing the IDs is discussed in the next subsection.

Hardy Wall Encryption Algorithm

The Hardy Wall Encryption Algorithm is designed using Fermat's Theorem. Algorithms based on Fermat's theorem are the most common for factorization.

The advanced method of factorizing multi-bit numbers is well explained by Mikolaj Karpinski [14] by using Fermat's Theorem. The formula generated for encrypting the device ID is stated in Equation 1.

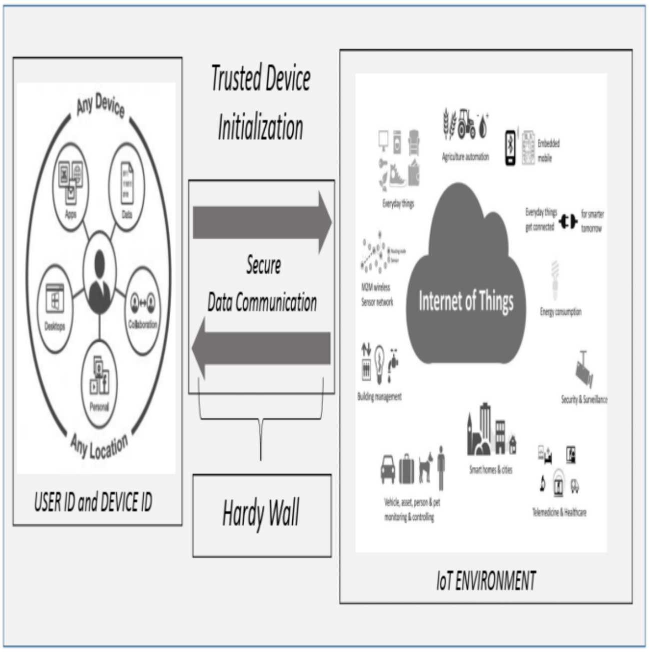


Fig. 1 Architecture of Proposed Model

$$HW= ((a \bmod b) / RN) + W + S \tag{1}$$

where: *HW – Hardy Wall Algorithm*
a – Alice Value
b – Bob Value
RN – Random Number
W – No. of Words
S – Sequence Number

The values of the "*k*" are substituted as in equation (2). Substituting the values in equation (2), equation (1) changes to equation (3)

$$(a \bmod b) = k \tag{2}$$

and

$$HW= (k / RN) + W + S \tag{3}$$

The entire working of Hardy Wall Encryption techniques is discussed though algorithm (1). The list of words of the user Id and the sequence number of the device ID is given as the input to the algorithm to obtain the best-encrypted device ID for secure transmission of the communication.

```
Input: List of Words W and Sequence Number S
Create a Hardy Wall HW to W and S
for each Words W and Sequence, Number S do
    Generate Alice value a, Bob Value b and
    Random Number RN
    Modulus a with b (a mod b) namely key K
    Divide K with RN (K/RN)
    Add (K/RN) with W and S
end for
If W and P is Encrypted E(W, S)
    Save E(W, S)
    Initialize the communication with E(W, S)
else
    Stop the initialization
end if
Output the best Encrypted formula
```

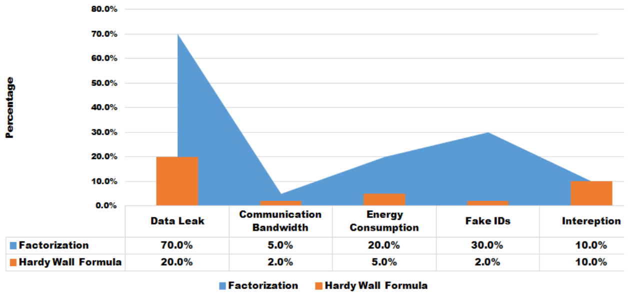
Algorithm 1: Hardy Wall Encryption Algorithm

IV. EXPERIMENTAL ANALYSIS

The experimental analysis was done for the proposed system by implementing in NS2 simulator. Various performance metrics were concerned for evaluating the model. Fig. 2 shows the various parameters considered for evaluation. The Hardy Wall Algorithm was compared with the traditional system which made use of factorization algorithm. By using the proposed algorithm it could be observed that the data leak occurring in the network has reduced to 20% from 80%. The communication bandwidth used by the system while using the factorization method was about 5% whereas, while using the Hardy Wall algorithm the network saw a decrease of 3% in the total communication bandwidth consumed. The energy consumption was minimized up to 15%. The main idea of the entire system is to identify the fake IDs and remove their access into the network. This idea was well achieved by the proposed system by limiting the number of fake Ids to about 2%.

Transmission speed is one the most vital requirement for a network. Be it, however, secure the network if the transmission speed is slow then the entire network fails to be implemented in real time. The networks need to be very fast in communicating with each other by exchanging messages and lack of this cannot build an efficient system. In Fig. 3 we have compared the transmission speed of the Hardy Wall Algorithm with the system using Fermat's Theorem. The Hardy Wall Algorithm has an overall transmission speed of about 80% which is only 50% while using Fermat's Theorem.

The overall weightage of the result and the formula are also compared for both the systems and it can be seen that thought the weightage of the formula is same, the result of the Hardy Wall Algorithm has observed to be greater than the Fermat's theorem.



	Data Leak	Communication Bandwidth	Energy Consumption	Fake IDs	Intereption
🟦 Factorization	70.0%	5.0%	20.0%	30.0%	10.0%
🟧 Hardy Wall Formula	20.0%	2.0%	5.0%	2.0%	10.0%

Fig. 2 Experimental Analysis of the Proposed Model

The system was built in various simulators and al the simulators had different strengths and its own weakness. While simulating the proposed system one of the major challenges faced was its memory size Simulators like OmNet++ and SimPy used the memory to a greater extent of about 140Mb and 100Mb

While using JiST the memory consumption was less to up to 80%. NS3 had the minimum memory consumption of about 60% and proved to be efficient for simulating the model to yield the best results. The comparison of the simulators used and the memory consumption of the simulators for running the proposed model is depicted in Fig. 3.

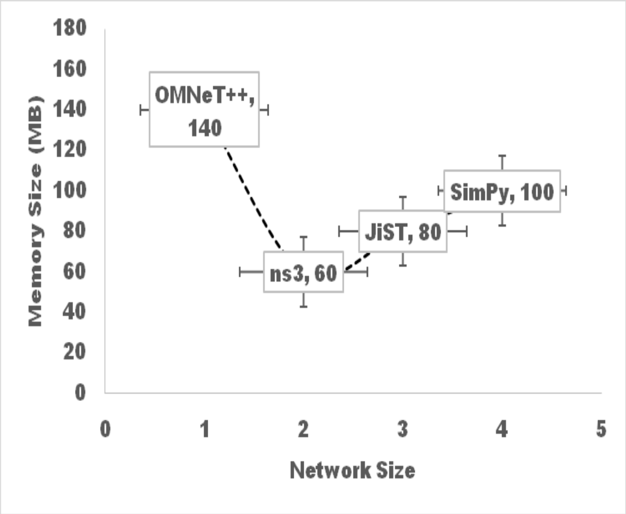


Fig. 3 Comparison of Memory size used in various Platforms

I. CONCLUSION

IoT plays a vital role in transmitting messages and communicating between various devices connected to the internet. Numerous services are used widely with the help of the IoT environment. The amount of information passed and stored in these networks are enormous and it is very essential to provide security to the data. Numerous researchers have worked on various fields to make the data secured within the environment. In this paper, we have proposed a Hardy Wall Algorithm that secures the device taking part in the transmission rather than securing the data being transmitted. All the devices connected to the network have their unique device ID and this ID is protected by using advanced mathematical cryptology. The proposed model is evaluated on various parameters such as the number of data leaks in the network, communication bandwidth and the existence of fake IDs in the network. It is observed that the proposed system outperforms the traditional systems and proves to use less memory space. The future work could include a combination of the proposed model with another mechanism that provides security to the data being transmitted. This would make both the data being transmitted and device through which the data is transmitted securely and thus provide an efficient model in an IoT environment.

respectively.

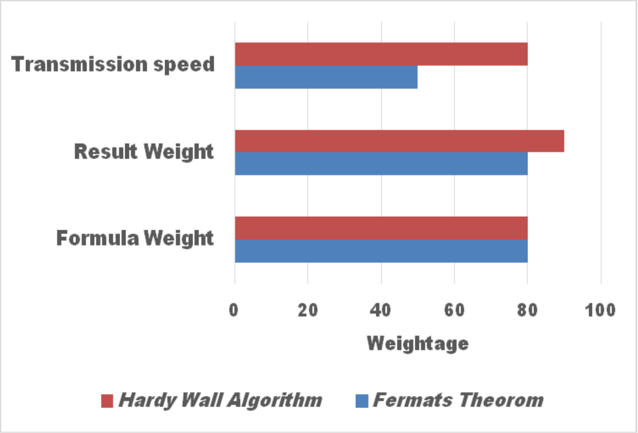


Fig. 3 Experimental Analysis of the Proposed Model

REFERENCES.

1. Khan, R., Khan, S. U., Zaheer, R., & Khan, S. (2012, December). Future internet: the internet of things architecture, possible applications, and key challenges. In Frontiers of Information Technology (FIT), 2012 10th International Conference on (pp. 257-260). IEEE.
2. Kawthankar, S., & Raut, C. (2017). A Survey on Smart Automobiles using the Internet of Things for Digital India. Transportation, 3(05).
3. Sheng, Z., Mahapatra, C., Zhu, C., & Leung, V. (2015). Recent advances in industrial wireless sensor networks towards efficient management in IoT. IEEE access, 3, 622-637.
4. Gope, P., & Hwang, T. (2016). BSN-Care: A secure IoT-based modern healthcare system using body sensor network. IEEE Sensors Journal, 16(5), 1368-1376.
5. Wang, M., Zhang, G., Zhang, C., Zhang, J., & Li, C. (2013, June). An IoT-based appliance control system for smart homes. In Intelligent Control and Information Processing (ICICIP), 2013 Fourth International Conference on (pp. 744-747). IEEE.
6. Ghazal, M., Hamouda, R., & Ali, S. (2015, October). An iot smart queue management system with real-time queue tracking. In e-Learning (econf), 2015 Fifth International Conference on (pp. 257-262). IEEE.
7. Medaglia, C. M., & Serbanati, A. (2010). An overview of privacy and security issues in the internet of things. In The Internet of Things (pp. 389-395). Springer, New York, NY.
8. Santoso, F. K., & Vun, N. C. (2015, June). Securing IoT for smart home system. In Consumer Electronics (ISCE), 2015 IEEE International Symposium on (pp. 1-2). IEEE
9. Memos, V. A., Psannis, K. E., Ishibashi, Y., Kim, B. G., & Gupta, B. B. (2018). An efficient algorithm for media-based surveillance system (EAMSuS) in IoT smart city framework. Future Generation Computer Systems, 83, 619-628.
10. Zhao, J. C., Zhang, J. F., Feng, Y., & Guo, J. X. (2010, July). The study and application of the IOT technology in agriculture. In Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on (Vol. 2, pp. 462-465). IEEE.

11. Van Kranenburg, R., & Bassi, A. (2012). IoT challenges. Communications in Mobile Computing, 1(1), 9.
12. Ammar, M., Russello, G., & Crispo, B. (2018). Internet of Things: A survey on the security of IoT frameworks. Journal of Information Security and Applications, 38, 8-27.
13. Zarpelão, B. B., Miani, R. S., Kawakani, C. T., & de Alvarenga, S. C. (2017). A survey of intrusion detection in Internet of Things. Journal of Network and Computer Applications, 84, 25-37.
14. Q. Jiang, J. Ma, F. Wei, Y. Tian, J. Shen, Y. Yang, An untraceable temporal-credential-based two-factor authentication scheme using ecc for wireless sensor networks, Journal of Network and Computer Applications 76.
15. Karpinski, M., Ivasiev, S., Yakymenko, I., Kasianchuk, M., & Gancarczyk, T. (2016, October). Advanced method of factorization of multi-bit numbers based on Fermat's theorem in the system of residual classes. In Control, Automation and Systems (ICCAS), 2016 16th International Conference on (pp. 1484-1486). IEEE.
16. Sh.T. Ishmukhametov, Methods for factorization of integers, Tutorial, Kazan University, Kazan, 2011.
17. Amin, R., Islam, S. H., Kumar, N., & Choo, K. K. R. (2018). An untraceable and anonymous password authentication protocol for heterogeneous wireless sensor networks. Journal of Network and Computer Applications, 104, 133-144.
18. Gandino, F., Ferrero, R., Montrucchio, B., & Rebaudengo, M. (2016). Fast hierarchical key management scheme with transitory master key for wireless sensor networks. IEEE Internet of Things Journal, 3(6), 1334-1345.
19. Hamid, M. A., Abdullah-Al-Wadud, M., Hassan, M. M., Almogren, A., Alamri, A., Kamal, A. R. M., & Mamun-Or-Rashid, M. (2018). A key distribution scheme for secure communication in acoustic sensor networks. Future Generation Computer Systems, 86, 1209-1217.
20. Li, X., Niu, J., Kumari, S., Wu, F., Sangaiah, A. K., & Choo, K. K. R. (2018). A three-factor anonymous authentication scheme for wireless sensor networks in internet of things environments. Journal of Network and Computer Applications, 103, 194-204.
21. Jiang, Q., Ma, J., Lu, X., & Tian, Y. (2015). An efficient two-factor user authentication scheme with unlinkability for wireless sensor networks. Peer-to-peer Networking and Applications, 8(6), 1070-1081.

AUTHORS PROFILE

M. Sundarrajan is currently pursuing his Ph.D. from Periyar Maniammai Institute of Science and Technology, Thanjavur, India. He had received his Master of Technology from SASTRA University, Thanjavur, India, and Bachelor of Engineering from PSV College of Engineering and Technology, Krishnagiri, India. He has good knowledge in the field of Internet of Things, Cyber-Physical System, Threat Intelligence and Data Security.

A.E. Narayanan has Received his Ph.D. from Periyar Maniammai University, Thanjavur, India. He had received his Master degree from Manonmaniam Sundaranar University, Tirunelveli, India, and Bachelor of Engineering from Government College of Technology, Coimbatore, India. His current research interests include Wireless Sensor Networks, Smart Grid, Cryptography, Internet of Things and Threat Intelligence.