A Light Weight Provenance Aware Trust Negotiation Algorithm for Smart Objects in IoT

J.A.D.C. Anuradha Jayakody[1], Lakmal Rupasinghe[2], N.T Mapa[3], T.S Disanayaka[4], D.S.A.Kandawala[5], K.D.Dinusha Chathurangi[6], Krishnadeva Kesavan[7]

Department of Information Systems Engineering, Sri Lanka Institute of Information Technology (SLIIT), Malabe, Sri Lanka.

[1] j.c.jayakody@postgrad.curtin.edu.au, [2] lakmal.r@sliit.lk, [3] navoda.m@sliit.lk [4], navoda.m@sliit.lk, [5] thushari.d@sliit.lk

ABSTRACT

Internet of Things can be considered as the next big tide which advances towards the ICT realm. Many research communities have shown enthusiastic interest towards the variety of research topics which has been emerged into a discussion related to this novel concept. The research taxonomy of IoT is built upon several key pillars by considering its Complexity, Heterogeneity, and Versatility nature. Among these, security related research challenges can be considered as a key impacting domain. This particular research has been conducted with the special consideration towards Trust Negotiation among smart objects in order to satisfy provenance related criteria. Therefore this paper has suggested a light –weight, less-complex, comprehensive encryption algorithm by applying shuffling techniques in order to satisfy the origin identification.

***Keywords*— Internet of Things (IoT), Security in IOT, Provenance, Trust Negotiation, Light – Weight Encryption**

1. INTRODUCTION

Current behavioral patterns depict that people around the world are more encourage towards consuming the services provided by the Internet to accomplish their day to day wants, needs and tasks. However, the resent observation represents an unprecedented consuming pattern with regards to the consumption of applications and services provided by the Internet. Based on the current context it is predictable that within the next years or decades to come the need of Internet-based services are going to be exceptionally high, and more people will be in the urge to access the global information contents. In such perspective, conventional methods will not be able to produce the expected outcomes that are been required. Therefore this eager to extend the interconnections has paved new ways to establish a big leap in the future of Internet. As a result, the concept of IOT has been emerging into the discussion.

IOT can be defined as an Umbrella concept which comprises all these desired aspects based on the paradigm of computing and communication. It has been built upon the idea, where the notion of interconnected smart devices acquire the main key objectives of anywhere - anytime - anything connectivity [2].

Since IOT can be defined as a futuristic technology trend, it consists of several challenging research domains [3].

Based on the considerations above the main scope of this investigation has been focused towards the role of the Security Domain in IoT. Since security, considerations has been a critical component it has been span across by reference to several research areas related to IoT. The following diagram depicts the taxonomy of the most demanded research areas relevant to the Security Domain of IoT.

Fig.1: Security in IoT

By reference to the context mentioned above, the core research focus of this paper has been narrowed down to the Trust based challenge objectives related to IoT. The follow- up content will clearly

clarify the actual need of embedding Trust into the IoT Infrastructure.

Internet of Things has been able to compose the technical and research savvy communities into diverse directions. The overall context of IoT comprises of an inter-connected, inter- related, the ever-growing system of physical objects, smart devices - embedded with electronics, software, and sensors.

The network connectivity which binds the entire IoT infrastructure thrives on a timely evolving spectrum of data collections generated by all most any object connected to the IoT network. These sets of data collections can be directed towards several stages of processing and ultimately can be manipulated in different ways by the application of particular logics. Ultimately the resulting Information Workflow can be used as the reference base in order to perform series of decision making related activities. Since the most vital attention has been focused towards the fetched data which is then directed towards into different levels of processing, ensuring the trustworthiness and the original ownership of the individual objects which produces the data has been a vital challenge. This particular objective has initiated the necessity of confirming certain level of data trust which can be reached by the application of the concepts related to Data Provenance. In order to ensure the provenance of an object, the object wise information extraction should be done at the initial point where the node was introduced to the IoT network base.

Based on the information above the base, the main objective of this research is to deliver a less-complex, light- weight trust negotiation algorithm to satisfy the requirement of provenance negotiation among the heterogeneous modes in IoT.

The remainder of the paper is organized as follows. In Section II, the paper has introduced and compared the different visions of the solutions available to the related subject, which is available from the literature. The system overview and the descriptive information about the proposed trust negotiation algorithm is presented subsequently in Section III and Section.

IV. The Final content Section V, concludes the paper and presents further extensions that could be performed which is aligned to the subject.

2. LITERATURE SURVEY

One of the most popular topics nowadays is Internet of Things (IoT) causes a high impact on several aspects of everyday life and behavior of potential users. Main advantage of the IOT is that it provides development of a huge number of applications in various domains such as

- Transportation and logistics domain.
- Healthcare domain.
- Smart environment (home, office, plant) domain.
- Personal and social domain [1].

Within this huge number of applications a wide range of individual objects identifiable via own IP addresses or similar identifier. Data provenance identifies the origin of data and processes operations on it will help to assure security requirements such as Integrity and Confidentiality of collecting data in the IoT. To get accurate trust level, several requirements need to be satisfied such as [2]:

- Completeness of Information
- Integrity
- Availability
- Confidentiality
- Efficiency
- Privacy
- Trust

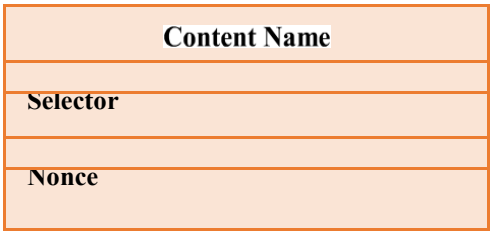
When it comes to the factor “Trust” it has a large number of Definitions and widely used definition is the one provided by Blaze and Feigenbaum, which refers to security policies regulating accesses to resources and credentials that are required to satisfy defined policies. At present a limited number of solutions available related to the identity management and access control issues. Most popular approaches include keynote and trust builder. However, any of these do not lend them to a straightforward application to the IOT domain due to high computational requirements that they impose [3]. In the paper of Javier Suarez, Jose Quevedo, Ivan Vidal, Daniel Corujo, Jaime Garcia-

Reinosa, Rui L. Aguiar on "A Secure IoT management architecture based on Information-Centric Networking" they had proposed a new architecture to improve trust between objects. According to them, it was a gargantuan challenge to develop an architecture which met all the requirements mentioned below.

- Scalability
- Energy Efficiency
- Self-organization
- Semantic Interoperability
- Privacy
- Security
- Computational ability of devices

Their architecture provides a generic and flexible platform that allows the appropriate operation of IoT devices with in a delimited ICN network domain, such as an organization or residential environment. Their design was designed to support a wide range of devices of different types and capabilities. The main component of their architecture is the gateway which acts as an intermediary communication element between clients and IoT devices. When it comes to the topic of discovery and registration of devices gateway, manually authenticate and configure the security mechanisms. In Object authentication procedure they have calculated a cryptographic digest of its public key, and a key locator, indicating where that public key can be obtained. The digital signature included by the gate way in data packets.

Interest Packet



Data packet

Fig.2: Data Packet and Interest packet

The encryption with the public key of the client used for ensuring a client is a legitimate object. When a client receives a data packet, client validates the digital signature and authenticate the gateway as the originator of the data packet and verify its Integrity [4].With the use of encryption mechanisms they have achieved the trust between objects

3. SYSTEM OVERVIEW

The concept of trust has divergent interpretations based on different contexts. Variety of definitions has been delivered on the adapted perspective. In the notion of IOT, still, there is no consensus definition related to the concept of trust even though its importance has been highly recognized. Since the peer – to – peer negotiation of different smart objects inside an IOT network is the key element to be established prior to establishing a communication session, ensuring it has been based on sensitive trust negotiation is a key point. This requirement leads to maintaining a mutual trust between the peer nodes of the IOT network. In order to perform such operation provenance, related information should be maintained in a proper way. The prevalent mechanism to perform such operation is by including the provenance information as an additional attribute to the routing information. Since provenance is concerned towards verifying the origin-related information of a smart node, the sensitivity of that information must be preserved. Therefore as means of persisting the provenance, this paper has suggested a Trust Negotiation mechanism focusing on Integrity constraint, by which the shared provenance information is protected from intruders. The structure of the proposed algorithm is described in the follow-up content.

Nodes which are willing to take part in the IOT network are configured with a key that is agreed upon the nodes. This pre-shared key is only known to the peer nodes. When the nodes need to exchange information via messages, the message proceeds through several steps. First of all the original message is taken. Then a random portion is selected out from the original message. The random selection depends on several characteristics of the same original message. Next, the message will be encrypted using a lightweight encryption algorithm by the use of shuffling mechanism and based on the set of properties related to the pre-shared key.

Finally, the shuffling algorithm produces the cipher text (Encrypted text) which is encapsulated in the message to be sent to the other side.

The receiving node takes the message and extract the cipher message portion and decrypt it with the pre-shared key in its possession. The integrity of the message is ensured if the received message portion and the decrypted message are matching with each other.

Comprehensive description of the aforementioned light- weighted encryption algorithm is presented in the next section.

4. SHUFFLING ALGORITHM

To apply shuffling algorithm following parameters need to be identified.

- Number of bits in the key
- No of zeros in the key bit stream
- No of ones in the key bit stream
- No of bytes in the message
- No of zeros in the randomly selected byte stream
- No of ones in the randomly selected byte stream

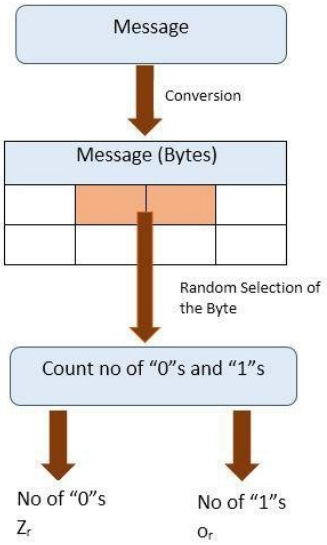


Fig.3: Shuffling algorithm's flow of counting 1's and 0's of message

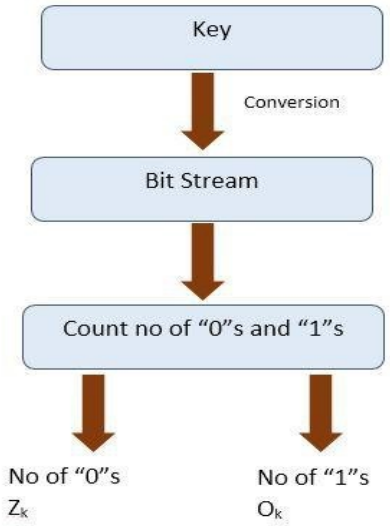


Fig.4: Shuffling algorithm's flow of counting 1's and 0's of key

When it comes to the random selection of the byte, the position of the byte is calculated using the following equation. In that case, we calculate the no of bytes in the message and divide it from the maximum no of zeros and number of ones.

RB - Random selection of the byte

N - No of bytes in the message

M - Max (number of ones, number of zeros)

$$RB = N / M \rightarrow (1)$$

Then we combine the no of zeros in randomly selected byte and key bit stream into a single parameter called " Z "and no of ones into a parameter called "O" using following equations.

Z - Combined number of zeros

Zr - Number of zeros in the key

Zk - Number of zeros in the random byte

$$Z = Zr + Zk \rightarrow (2)$$

O - Combined number of zeros

Or - Number of zeros in the key

Ok - Number of zeros in the random byte

$$O = Or + Ok \quad (3)$$

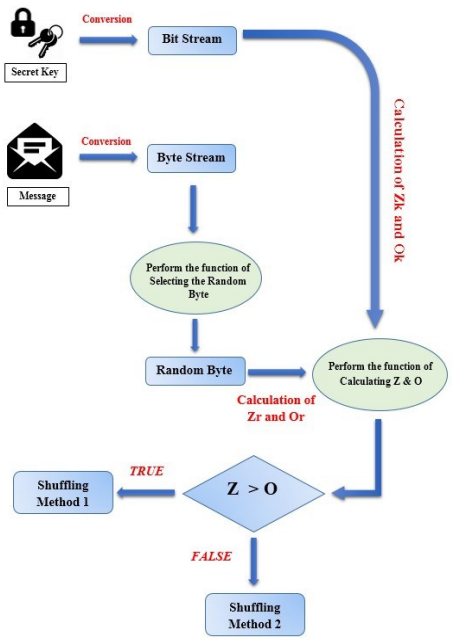


Fig.5: Flow of Shuffling Algorithm

The shuffling method will be selected after performing the function of calculating Z and O. If Z>O then the shuffling method 1 will be used. Else method 2 will be used.

A. Shuffling Process: Method 1

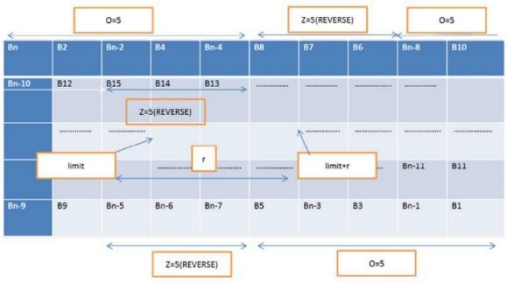


Fig.6: Example of Method 1

Here for "O" number of bytes we interchange the bytes with the last "O" number of bytes. We take "Z" number of bytes after the "O" number of bytes and reverse them in both front and the back of the message. Likewise, we continue the process until we meet a limit which is denoted by the variable "limit". Here we assume that "Z" is equal to 3 and "O" is equal to 5.

A. Shuffling Process: Method 2

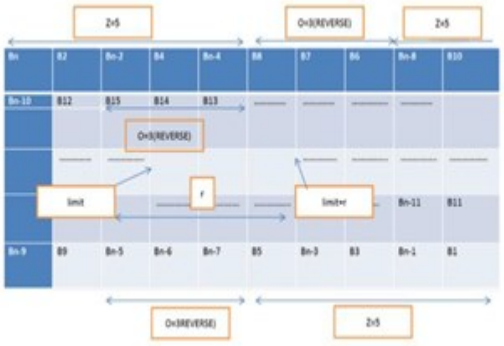


Fig.7: Example of Method 2

Here for "Z" number of bytes we interchange the bytes with last corresponding "Z" number of bytes. We take "O" number of bytes after the "Z" number of bytes and reverse them in both front ends the back ends of the message. Likewise, we repeat the process until we meet the variable "limit." Here we assume that "Z" is equal to 5 and "O" is equal to 3.

The "Limit" variable will be calculated using the following equation.

$$Limit = (tb / (O+Z)*2))*(O+Z) \longrightarrow (4)$$

Above given equation (4) will be calculated based on integer division. The parameter "tb" is calculated relative to the length of the message (tb = message.length ()).

5. CONCLUSION AND FUTURE WORK

Nodes which exists in an IoT shows versatile characteristics due to its heterogeneous nature. This requirement has led to ensuring a certain level of origin based trust related to the associated network. Trust Negotiation among the smart nodes has always been a challenging goal since the devices present are equipped with different levels of power and computational capabilities. Based on these key factors this research paper has presented a light-weight, less- complex trust negotiation algorithm with the application of simple shuffling mechanisms. When the focus is extended towards the future, the structure of the algorithm can be further optimized to achieve less computational and fewer power consumptions patterns.

6. ACKNOWLEDGEMENTS

This work has been supported by Sri Lanka Institute of Information Technology, Malabe, Sri Lanka.

7. REFERENCES

[1] Luigi Atzori a, Antonio Iera b, Giacomo Morabito c, "The Internet of Things: A survey", DIEE, University of Cagliari, Italy, University ''Mediterranea" of Reggio Calabria, Italy, University of Catania, Italy, 2012.

[2] Sabine Bauer, "Data Provenance in the Internet of Things", IT-Security Group, University Passau, 2013.

[3] Daniele Miorandi , Sabrina Sicari , Francesco De Pellegrini , Imrich Chlamtac "Internet of things: Vision, applications and research challenges", in International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, Int. Conf., 2013.

[4] Javier Suarez,Jose Quevedo,Ivan Vidal,Daniel Corujo,Jaime Garcia- Reinoso,Rui L.Aguiar., "A Secure IoT management architecture based on Information –Centric Networking", University of Journal of Network and Computer Applications, 2016.

[5] John A. Stankovic," Research Directions for the Internet of Things"Computer. Sci. Dept., Univ. of Virginia, Charlottesville, VA, USA,2014

[6] "The Internet of Things: An Overview", 2015. [Online].Available:https://www.internetsociety.org/sites/default/files/ISOC-IoT-Overview-20151014_0.pdf

[7] Friedemann Mattern and Christian Floerkemeier," From the Internet of Computers to the Internet of Things",2009

[8] "Internet of Things", 2015.[Online].Available:http://www.cisco.com/c/en/us/solutions/internet-of-things/overview.html

[9] Ala Al-Fuqaha et-al," Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications", 2015

[10] "Security In The Internet Ofthings",2015.[Online].Available:http://www.windriver.com/whitep apers/security-in-the-internet-of-things/wr_security-in-the-internet-of- things.pdf

[11] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," Comput. Netw. vol. 54, no. 15, pp. 2787–2805, Oct. 2010.

[12] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future Internet: The Internet of Things architecture, possible applications and key challenges," in Proc. 10th Int. Conf. FIT, 2012, pp. 257–260.

[13] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): vision, architectural elements, and future directions," Future Gener. Comput. Syst., vol. 29, no. 7, pp. 1645–1660, Sep. 2013.

[14] P. Lopez, D. Fernandez, A. J. Jara, and A. F. Skarmeta, "Survey of Internet of Things technologies for clinical environments," in Proc. 27th Int. Conf. WAINA, 2013, pp. 1349–1354.

[15] D. Yang, F. Liu, and Y. Liang, "A survey of the Internet of Things," in Proc. 1st ICEBI, 2010, pp. 358–366.

[16] A. Gluhak et al., "A survey on facilities for experimental Internet of Things research," IEEE Commun. Mag., vol. 49, no. 11, pp. 58–67, Nov. 2011.

[17] Z. Sheng et al., "A survey on the IETF protocol suite for the Internet of Things: Standards, challenges, and opportunities," IEEE Wireless Commun., vol. 20, no. 6, pp. 91–98, Dec. 2013.

[18] J. Gantz and D. Reinsel, "The digital universe in 2020: Big data, bigger digital shadows, and biggest growth in the Far East," IDC iView: IDC Anal. Future, vol. 2007, pp. 1–16, Dec. 2012.

[19] M. Wu, T. J. Lu, F. Y. Ling, J. Sun, and H. Y. Du, "Research on the architecture of Internet of Things," in Proc. 3rd ICACTE, 2010, pp. V5- 484–V5-487.

[20] EU FP7 Internet of Things Architecture Project, Sep. 18, 2014. [Online]. Available: http://www.iot-a.eu/public