International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 07
June 2019

External Reliability and Data Source Communication Using Semantic Web of Things

[1]Thatiparthi Rajini, [2]Dr.P.Pedda Sadhu Naik

Abstract: With the dawn of autonomous organization and network and service management, the integration of existing networks with Internet of Things (IoT) based networks is becoming a reality. The interconnection of resource-constrained and globally accessible things with untrusted and unreliable Internet make them vulnerable to attacks including data forging, false data injection, and packet drop that affect applications with critical decision-making processes. We propose a novel lightweight scheme to securely transmit provenance for sensor data. The proposed technique relies on in packet Bloom filters to encode provenance. We introduce efficient mechanisms for provenance verification and reconstruction at the base station. Our approach uses packet Bloom filters that are encoded as sensor data travels via intermediate sensor nodes, and are decoded and verified at the Receiver. Thus Information Gain by Receiver will Trace out the data Path through which it comes. Noteworthy efforts in overcoming unpredictability (particularly in case of large dimensions) are the ones integrating Knowledge Representation technologies to build the so called Semantic Web of Things (SWoT). n. This paper proposes a novel Service-Oriented Architecture (SOA) based on a semantic block chain for registration, discovery, selection and payment. We introduce efficient mechanism ms for provenance verification and reconstruction at the base station. In addition, we extend the secure provenance scheme with functionality to detect packet drop attacks staged by malicious data forwarding nodes. We evaluate the proposed technique both analytically and empirically, and the results prove the effectiveness and efficiency of the lightweight secure provenance scheme in detecting packet forgery and loss attacks.

Index Terms: Provenance, security, sensor networks, Semantic Web, Internet of Things, Matchmaking, Ubiquitous Computing, Bloom Filter Packet generation, Fault location. Security, Sensor Networks.

1. INTRODUCTION

Sensor systems are utilized as a part of various application spaces digital physical foundation frameworks, natural observing, power networks, and so on. Data are conveyed considerable number of sensor center point sources and arranged in framework at widely appealing skips way to base stations perform essential authority [1]. The trust of transactions in the digital world is strictly related to the confidence on a given authority it has to be noticed that today the assets made in a virtual way are more and more increasing [2]. Our provenance approach uses light-weight in-packet Bloom filters that are encoded as device information travels through intermediate device nodes, and are decoded and verified at the bottom station is additionally able to defend against malicious attacks like packet dropping and permits one to sight the accountable node for packet drops [3]. Provenance must be recorded for each packet, but important challenges arise due to the tight storage, energy and bandwidth constraints of sensor nodes [4]. To enforce trustworthy data in transit and routing with quality of services (QoS), it is essential to keep track of the complete data propagation path. Such tracking of data can be formulated through Provenance [5]. We used cipher-text-policy attribute-based encryption (CP-ABE) [14] instead of Public key Cryptography for designing our secure provenance mechanism the authors have discussed how the algorithm of CP-ABE can be distributed [6]..

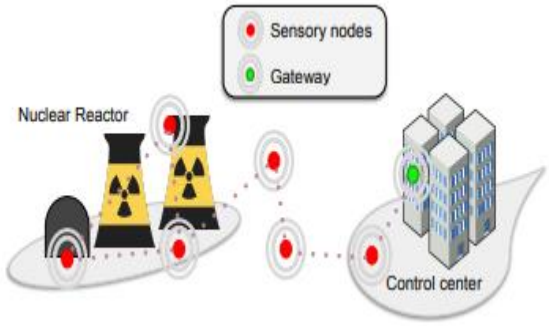

Fig. 1: Nuclear reactor scenario sensory nodes relaying data

2. RELATED WORK

Data provenance provides the source of information and the historical path it has been forwarded from. Scientist is interested in the origin and historical transformation of the data as it contains critical information about the reliability of the data [7]. In smart cities, sensors can be deployed in many sectors including monitoring crops for precision agriculture, traffic analysis, environmental monitoring, energy management, identifying parking spaces, health care, food quality, and many others sensors to control and

automate the daily life activities [8]. We do not consider denial of service attacks such as the complete removal of provenance, since a data packet with no provenance records will make the data highly suspicious and hence generate an alarm at the BS [9]. This paper proposes meta-knowledge metaphysics to align the ideas and properties of existing root age schemas and ontology's. The meta-provenance metaphysics permits common interpretation of various provenances, and thus their integration [10]. SWoT opens the way toward an ontology-based resource/service discovery leveraging semantics of requests and resource descriptions to refine retrieval strategies [11]. The proposed technique realizes upon pack bloom channels encode provenance, so present profitable segments for provenance check and remarking at base hub. Furthermore it expand the safe provenance plan with usefulness to distinguish bundle drop assaults tagged by noxious information sending hubs and the outcomes demonstrate the adequacy and productivity of the lightweight secure provenance plan in recognizing parcel fraud and misfortune assaults [12]..

3. SYSTEM ARCHITECTURE

The source node sends the request to neighboring nodes in the network to find the shortest path for sending secure provenance transmission in sensor networks, and identify in-packet Bloom filter (iBF) provenance encoding scheme and efficient techniques for provenance decoding and verification at the base station [13]. Concept expressions can be used in inclusion and definition axioms, which model knowledge elicited for a given domain [14]. Thus, transcription location-sensitive peer-to-peer storage is one challenge. Device information sets don't have obvious names, therefore naming them during a globally helpful fashion is another challenge [15]. We consider for our proposed provenance scheme for RPL networks. We also present the provenance model along with the outline of elemental provenance data components that are utilized in our proposed scheme [16].

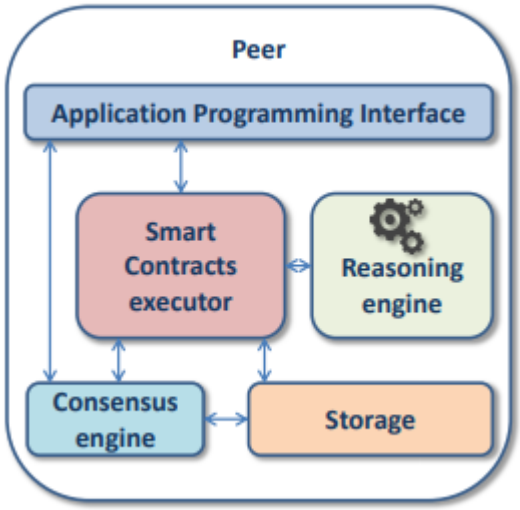

Figure 2: Framework architecture

4. PROPOSED SYSTEM

We have a tendency to present associate degree economical and secure approach for sending origin info concerning sensing element knowledge. Our provenance approach uses light-weight in-packet Bloom filters that are encoded as sensing element knowledge travels through intermediate sensing element nodes, and are decoded and verified at the bottom station [17]. During the process of network operations only is considered to be a trusted entity. An adversary in the network may compromise other benign nodes [18]. Cloud environment new devices connected to the cloud edge nodes would be assigned that would be closed to the devices as compared to the main servers of the Cloud [19].

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 07
June 2019

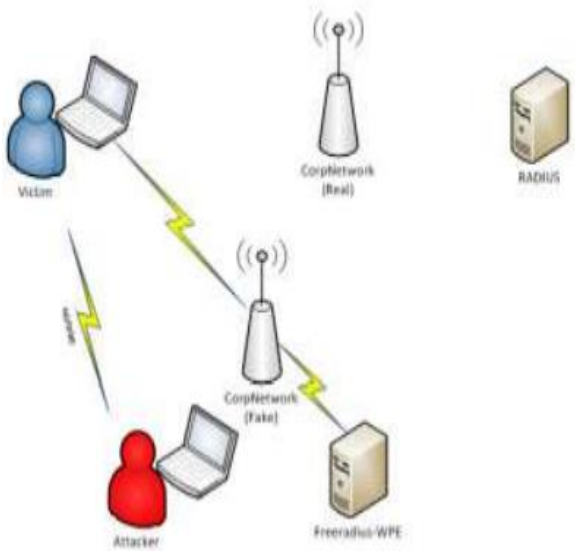

Fig.2. Attacker attacks the Data Nodes

A. Secure Provenance based on CP-ABE

For securing the provenance mechanism, Cipher text-Policy Attribute based Encryption (CP-ABE) is used the conceptual model of implementing the CP-ABE in Cloud environment. The distribution of CP-ABE algorithm is adopted from where the authors have implemented the load sharing of cryptographically computation by outsourcing the signing and signature verification to the edge nodes. [20].

These five steps is Setup, Key Generation, Signing-outsourced and Signing. Signing outsourced has most of the computational load that is why it is performed by the fog/edge node, while the step with significantly lower overhead, i.e. Signing is performed details of each step are as follows:

CP-ABE Algorithm

1) **Setup:** this step is the first step which is performed at the attribute authority node, or the edge node.
2) **Key Generation:** This is the second step, which is to be performed by the attribute authority process of signing by requesting the attribute authority for secret key for the node with attribute set
3) **Sign Outsourced:** This phase is executed by the edge/fog attribute set and node, which takes input the secret key The CP-ABE is used to create the partial signature partial signature is calculate the final signature and the computational overhead is bared by the edge/fog node.
4) **Sign:** After the message is signed node, the message is forwarded to the next node. The signature message includes the identity of the sender, the identity of the forwarding node and the original data of the node is attached to verify if there was a by an adversary node.
5) **Verify:** The verify phase takes input the message the verification process secure provenance mechanism can identify the break in provenance chain. It would ask the sender node to resent the data.

B. Bloom-Filter

BF is a space effective information structure for probabilistic representation of an arrangement of things S = {s1, s2, . . . sn} utilizing a variety of bit with k free hash capacities yield every hash capacity hey map a thing s consistently reach The BF can be spoken to as {b0, . . . bm_1}. At first all bit are set to zero. Embed a component s ∈ S into BF, s is hashed with all k capacities creating qualities hi(s) ($1 \leq i \leq$ k).bit relating to qualities exhibit [21]. On the off chance that any of them is 0, then surely s/∉ S. Something else, on the off chance that the majority of the bit is set to 1, sl∉ S high likelihood here exists a probability of blunder which emerges because of hashing crash that makes the components in S on the whole creating files hi(s/) being set to 1 regardless of the fact that s/∉ S. This is known as false positive

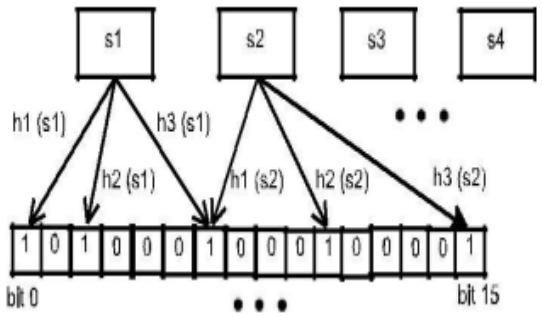

Fig5.3. Sprout channel

5. **SECURE PROVENANCE ENCODING**:

We propose a distributed mechanism to encrypt provenance at the nodes and a centralized formula to decipher it at the BS. The technical core of our proposal is that the notion of in packet Bloom filters

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 07
June 2019

(iBF). every packet consists of a novel sequence range, data value associated an iBF that holds the place of origin. we tend to emphasize that our focus is on firmly sending cradle to the BS [22].

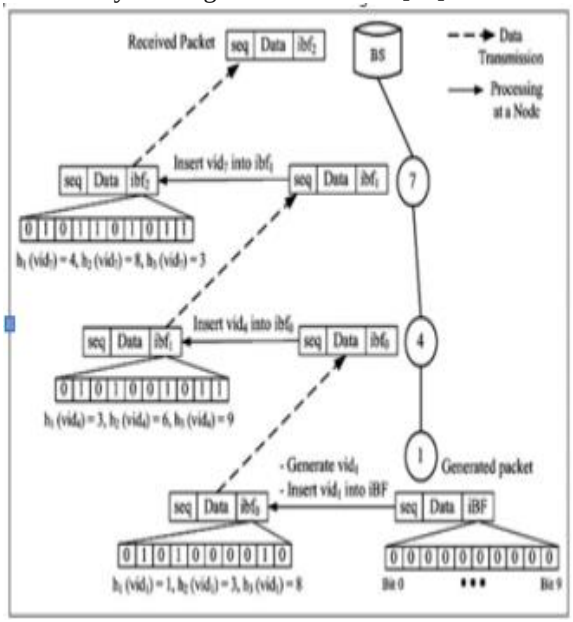

Fig.4. System for encoding provenance

6. RES ULTS & DISCUSSION

This work focused on obtaining maximum life time of the network. The source node sends the data to neighboring nodes in the network. In order to obtain a quantitative performance analysis of the proposed framework, various parameters were measured and evaluated. Small, medium and large scale scenarios were considered, respectively nodes. The computational load measurement of the proposed scheme for performing key generation and signature with the support of the edge node and without the support of edge node hence, the battery drainage issue can also be resolve using outsourced signature technique.

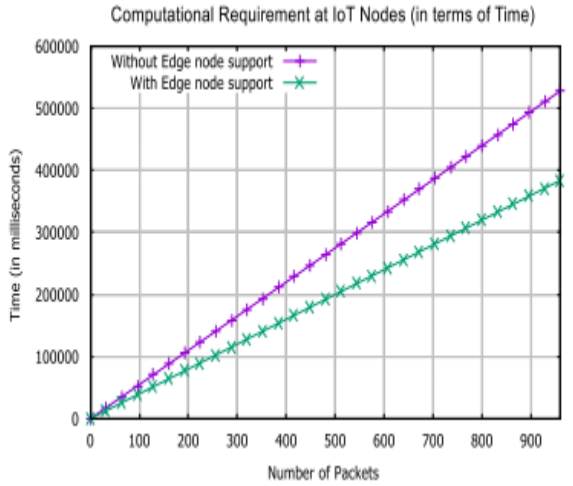

Fig. 5. Time Required to Generate Key and Signature Computation

7. CONCLUSION AND FUTURE WORK

We have proposed a secure provenance tracking mechanism which uses the outsourced signing technique using Attribute Based Encryption by offloading the node. We have introduced node-level provenance by embedding sequence number against routing entry at the routing table of the respective forwarding node. We extended the scheme to incorporate data-provenance binding, and to include packet sequence information that supports detection of packet loss attacks. The theme ensures confidentiality integrity and freshness of sensing element information. We tend to embody packet sequence data that supports detection of packet loss attacks. An important feature of the proposal resides on the logic-based explanation of discovery outcomes, obtained through non-standard inference for matchmaking among request and resources. Future work will be essentially scheduling tool in cluster computing environments, in order to increase the simulation scale of several order of magnitude nodes. We are also investigating for a possible solution using Block chain technologies, which has inherent characteristics to sim in data provenance.

8. REFERENCES

[1] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in internet-of-things," IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1250–1258, Oct 2017.

[2] Chen, Xiaofeng, "Secure Outsourced Attribute-Based Signatures", IEEE transactions on parallel and

distributed systems, 2014, Volume: 25 Issue: 12 Page: 3285-3294
[3] Sabah Suhail, Zuhaib Uddin Ahmad, Choong Seon Hong, "Introducing Secure Provenance in IoT: Requirements and Challenges" International Workshop on Secure Internet of Things (SIoT 2016), Sep. 26-30, 2016, Heraklion, Crete, Greece
[4] Peter Buneman, Sanjeev Khanna, and Wang Chiew Tan. Data provenance: Some basic issues. In Proceedings of the 20th Conference on Foundations of Software Technology and Theoretical Computer Science, FST TCS 2000, pages 87–93, London, UK, UK, 2000. Springer-Verlag
[5] Pasquier, Thomas; Lau, Matthew K.; Trisovic, Ana; Boose, Emery R.; Couturier, Ben; Crosas, Mercè; Ellison, Aaron M.; Gibson, Valerie; Jones, Chris R.; Seltzer, Margo (5 September 2017). "If these data could talk". Scientific Data. 4: 170114. doi:10.1038/sdata.2017.114.
[6] Robert Ikeda and Jennifer Widom. Data lineage: A survey. Technical report, Stanford University, 2009.
[7] Y. Cui and J. Widom. Lineage tracing for general data warehouse transformations. VLDB Journal, 12(1), 2003.
[8] Muhammad Naveed Aman, Kee Chaing Chua, Biplab Sikdar, Secure Data Provenance for the Internet of Things, Proceedings of the 3rd ACM International Workshop on IoT Privacy, Trust, and Security, April 02- 02, 2017, Abu Dhabi, United Arab Emirates
[9] Bilal Shebaro, Salmin Sultana, Shakthidhar Reddy Gopavaram, and Elisa Bertino. Demonstrating a lightweight data provenance for sensor networks. In Proceedings of the 2012 ACM conference on Computer and communications security, pages 1022–1024. ACM, 2012.
[10] Salmin Sultana, Mohamed Shehab, and Elisa Bertino. Secure provenance transmission for streaming data. IEEE Transactions On Knowledge And Data Engineering, 25(8):1890–1903, 2013.
[11] Salmin Sultana, Gabriel Ghinita, Elisa Bertino, and Mohamed Shehab. A lightweight secure scheme for detecting provenance forgery and packet dropattacks in wireless sensor networks. IEEE Transactions on Dependable and Secure Computing, 12(3):256–269, 2015
[12] M. Garofalakis, J. Hellerstein, and P. Maniatis, “Proof sketches: Verifiable in-netwok aggregation,” in ICDE, 2007, pp. 84–89.
[13] T. Wolf, “Data path credentials for high-performance capabilitiesbased networks.” in Proc. of ACM/IEEE Symp. on Architectures for Networking and Communications Systems., 2008, pp. 129–130.
[14] H. Chan, A. Perrig, and D. Song, “Secure hierarchical in-network aggregation in sensor networks,” in Proc. of the conf. on Computer and communications security (CCS), 2006, pp. 278–287.
[15] S. Roy, M. Conti, S. Setia, and S. Jajodia, “Secure data aggregation in wireless sensor networks,” IEEE Transactions on Information Forensics and Security, vol. 7, no. 3, pp. 1040–1052, 2012.
[16] C. Karlof and D. Wagner, “Secure routing in wireless sensor networks: attacks and countermeasures,” in Proc. of Intl. Workshop on Sensor Network Protocols and Applications, 2003, pp. 113–127.
[17] S. Marti, T. J. Giuli, K. Lai, and M. Baker, “Mitigating routing misbehavior in mobile ad hoc networks,” in Proc. of the Intl. Conf. on Mobile Computing and Networking, 2000, pp. 255–265.
[18] M. Ruta, E. Di Sciascio, and F. Scioscia, “Concept Abduction and Contraction in Semantic-based P2P Environments,” Web Intelligence and Agent Systems, vol. 9, no. 3, pp. 179–207, 2011.
[19] F. Scioscia and M. Ruta, “Building a Semantic Web of Things: Issues and Perspectives in Information Compression,” in Semantic Web Information Management (SWIM’09). In Proceedings of the 3rd IEEE International Conference on Semantic Computing (ICSC 2009), 2009, pp. 589–594.
[20] F. Scioscia, M. Ruta, G. Loseto, F. Gramegna, S. Ieva, A. Pinto, and E. Di Sciascio, “A Mobile Matchmaker for the Ubiquitous Semantic Web,” International Journal on Semantic Web and Information Systems (IJSWIS), vol. 10, no. 4, pp. 77–100, 2014.
[21] A. Ramachandran, K. Bhandankar, M. Tariq, and N. Feamster, “Packets with Provenance,” Technical Report GTCS-08-02, Georgia Tech, 2008
[22] W. Zhou, M. Sherr, T. Tao, X. Li, B. Loo, and Y. Mao, “Efficient Querying and Maintenance of Network Provenance at Internet- Scale,” Proc. ACM SIGMOD Int’l Conf. Management of Data, pp. 615-626, 2010.

Authors Details:

Thatiparthi Rajini
Mail id:rajini.thatiparthi4u@gmail.com

Dr.Samuel George Institute of Technology, Markapur, AP.

Dr.P.Pedda Sadhu Naik, Professor & HOD, Dr.Samuel George Institute of Technology, Markapur, AP.