ENSURING DATA SECURITY AND PRIVACY FOR THE INTERNET OF THINGS

SRIMATHI KESHETTI[1],MUTHAIAH THUMMA[2]
[12]Assistant Professor
Department Of CSE
Sree Chaitanya College of Engineering, Karimnagar

ABSTRACT :

The Internet of Things, or IoT, has been rapidly developing in recent years as a crucial component of the Internet of the future. IoT devices improve people's lives, but they also create and collect vast amounts of data that may be used for a variety of purposes by machine learning and big data analytics. Data security and privacy are critical concerns that must be addressed to prevent various cyberattacks (such as impersonation and data pollution/poisoning assaults) because of the machine-to-machine (M2M) communication nature of the Internet of Things. However, creating adaptable and lightweight IoT security solutions is a difficult task given the limited processing power and variety of IoT devices. In this research, we offer an IoT message authentication technique that is secure, private-preserving, and efficient. Our technique is more flexible and effective than the previous alternatives since it supports IoT devices with various cryptographic setups and enables for offline/online computing.

DOI Number: 10.48047/NQ.2022.20.12.NQ77765 NeuroQuantology2022;20(12): 4400-4406

I. INTRODUCTION :

The Internet of Things (IoT) provides a self-establishing network of highly coupled heterogeneous objects, such as smart devices, RFID tags, sensors, etc. It allows devices to simplify the retrieval as well as the exchange of data without human involvement in various applications [1] and has a considerable position in the growth of information technology after the computer science and the Internet. IoT brings a pervasive digital appearance by engaging society and industries, and enables a series of interactions between human to human, human to thing, and more importantly, thing to thing. The development of IoT has led to enormous applications, such as smart home systems (SHSs) [2], intelligent transportation systems [3][4], machine learning and big data [5], etc. The machine-to-machine (M2M) [6] communication among massive numbers of IoT devices will dominate future communication network traffic. The integrity and authenticity of the massive amount of data collected and transmitted by the IoT devices are crucial in some applications such as machine learning and big data analytics. Maliciously injected or modified data can cause biased or wrong decision making and prediction. Therefore, in order to ensure the correctness and accuracy of machine learning and big data analysis, the integrity and authenticity of the collected data must be retained [7].

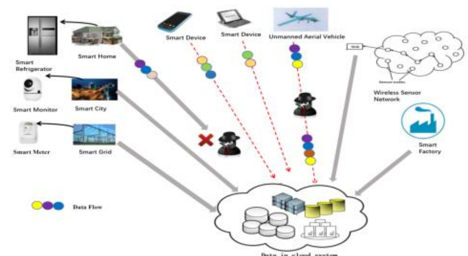
There are two approaches to achieve secure message delivery in IoT: the symmetric-key based approach, and the publickey based approach. The symmetric-key approach incurs less computation overhead compared with the public-key approach since symmetric-key operations are much more efficient than their public-key counterparts. However, key management is a major issue for symmetric-key based approach in a large scale heterogeneous IoT network. Also, if the message is only authenticated using a shared key between the sender and the receiver, the intermediate forwarding nodes in the IoT network cannot verify the integrity of the message. If the message has been altered or damaged during transmission, then the problem can only be discovered by the receiver. On the other hand, public-key based approach can solve these problems since anyone can use the public key to verify the integrity and authenticity of a message. However, public-key operations are very computation intensive, and privacy is another concern for public-key based approach since the authentication token is publicly verifiable using the sender's public key. It is worth noting that the privacy of a data source is also important in some situations, e.g., when a wearable device is attached to a human. If the attacker can identify the sources of the data streams, then they could also cut off a data stream (e.g., via a Denial-of-Service attack) and eventually affect the accuracy of the decision or prediction produced by machine learning.

In order to address the above problems in IoT and M2M communications, a secure, efficient and privacy-preserving message authentication scheme that can support hop-by-hop verification is desirable. In [8], Li et al. proposed a novel source anonymous message authentication (SAMA) scheme which could be used for such a purpose. Their scheme was believed to achieve message authentication and message source privacy with a lower cost than the previous approaches.

PROBLEM STATEMENT :

There are two approaches to achieve secure message delivery in IoT: the symmetric-key based approach, and the publickey based approach. The symmetric-key approach incurs less computation overhead compared with the public-key approach since symmetric-key operations are much more efficient than their public-key counterparts. However, key management is a major issue for symmetric-key based approach in a large scale heterogeneous IoT network. Also, if the message is only authenticated using a shared key between the sender and the receiver, the intermediate forwarding nodes in the IoT network cannot verify the integrity of the message. If the message has been altered or damaged during transmission, then the problem can only be discovered by the receiver. On the other hand, public-key based approach can solve these problems since anyone can use the public key to verify the integrity and authenticity of a message. However, public-key operations are very computation intensive, and privacy is another concern for public-key based approach since the authentication token is publicly verifiable using the sender's public key. It is worth noting that the privacy of a data source is also important in some situations, e.g., when a wearable device is attached to a human. If the attacker can identify the sources of the data streams, then they could also cut off a data stream (e.g., via a Denial-of-Service attack) and eventually affect the accuracy of the decision or prediction produced by machine learning.

MODEL DIAGRAM :



II. LITERATURE SURVEY

TITLE :

Internet of things in industries: A surve

AUTHORS :

G. Wettstein, J. Grosen, and E. Rodriguez

ABSTRACT:

Internet of Things (IoT) has provided a promising opportunity to build powerful industrial systems and applications by leveraging the growing ubiquity of radio-frequency identification (RFID), and wireless, mobile, and sensor devices. A wide range of industrial IoT applications have been developed and deployed in recent years. In an effort to understand the development of IoT in industries, this paper reviews the current research of IoT, key enabling technologies, major IoT applications in industries, and identifies research trends and challenges. A main contribution of this review paper is that it summarizes the current state-of-the-art IoT in industries systematically.

TITLE :

A nonce-based protocol for multiple authentications

AUTHORS :

A. Kehne, J. Schonwalder, and H. Langendorfer

ABSTRACT:

MIT's Project Athena, is based on the Needham and Schroeder protocol. Timestamps depending on reliable synchronized clocks are used to guarantee the freshness of messages. As an improvement, we present a nonce-based protocol offering the same features as Kerberos. We generate a ticket in an initial message exchange which includes a generalized timestamp. Checking this generalized timestamp is left to the principal who created it. Consequently we do not need synchronized clocks. Our protocol has the property of using a minimal number of messages to establish an authenticated session key.

TITLE :

A privacy preserving communication protocol for iot applications in smart home

AUTHORS :

T. Song, R. Li, B. Mei, J. Yu, X. Xing, and X. Chen

ABSTRACT:

The development of the Internet of Things has made extraordinary progress in recent years in both academic and industrial fields. There are quite a few smart home systems (SHSs) that have been developed by major companies to achieve home automation. However, the nature of smart homes inevitably raises security and privacy concerns. In this paper, we propose an improved energy-efficient, secure, and privacy-preserving communication protocol for the SHSs. In our proposed scheme, data transmissions within the SHS are secured by a symmetric encryption scheme with secret keys being generated by chaotic systems. Meanwhile, we incorporate message authentication codes to our scheme to guarantee data integrity and authenticity. We also provide detailed security analysis and performance evaluation in comparison with our previous work in terms of computational complexity, memory cost, and communication overhead.

III. SYSTEM ANALYSIS

EXISTING SYSTEM :

In order to prevent various types of attacks in data transmission, both symmetric-key and public-key approaches have been proposed in the literature. In [12], two different message authentication protocols were proposed. The first protocol, named TESLA, is based on Message Authentication Code (MAC), and the design utilizes a one-way key chain and timed release of keys by the sender. However, the TESLA protocol requires synchronization among devices, which is difficult to implement in a large scale network. The second protocol in [12], named EMSS, is based on cryptographic hash function and public-key technique, and can achieve the security property of non-repudiation. In [13], an interleaved hop-by-hop authentication scheme was proposed to prevent the injected false data packet attack by attackers or compromised nodes in the network. Their scheme is symmetric-key based, and the basic idea is that multiple sensor nodes have to endorse a message (or report) using MACs in order to achieve message authentication. A similar approach was also proposed in an independent work by Ye et al. [14]. In [15], a polynomial based approach was proposed to achieve lightweight and compromise-resilient message authentication, where messages are authenticated and verified via evaluating polynomials. In [8], Li et al. proposed a ring signature [16] based solution to achieve message authentication. Their scheme utilizes a ring signature scheme derived from the modified ElGamal signature scheme [10], and can achieve better features and performance in several aspects compared with the previous solutions. However, as we will demonstrate later, the ring signature scheme proposed in [8] has a security flaw: it allows an attacker to arbitrarily form a ring and forge a valid ring signature from an existing one. Such an attack has been considered in the literature of ring signature (e.g., [17]) and in this work we introduce a technique similar to that of [17] to fix the flaw without introducing any computation or communication overhead.

There are also a number of research works on privacy preserving user authentication (and key agreement) protocols for IoT and wireless sensor networks (WSNs) in recent years (e.g., [18], [19], [20], [21], [22], [23], [24], [25], [26]). These works focus on remote user authentication, which is related but different from the privacy preserving hop-by-hop message authentication considered in this paper. Moreover, due to the concerns on the physical security of sensor nodes and IoT devices, the research on constructing lightweight and physically secure authentication protocols for IoT and wireless sensor networks has also become a popular topic in recent years. To ensure physical layer security, Physically Unclonable Functions (PUFs) and wireless channel characteristics (such as the Link Quality Indicator (LQI)) are popular choices to enable security even if a sensor node is captured by an adversary. Several novel lightweight authentication protocols with physical security for IoT and WSNs can be found in [27][28][29].

DISADVANTAGES OF EXISTING SYSTEM :

1) Less accuracy
2)low Efficiency
3) he system is less effective due to lack of source location privacy
4) The system has only detection techniques and no protection techniques.

PROPOSED SYSTEM :

Moreover, considering the low computation power of the IoT devices, we also apply the offline/online paradigm in the design of our system. Efficiency is extremely important in practical IoT scenarios such as industrial automation, environmental monitoring, smart grids, etc. In proposed scheme, a smart device can perform some expensive public-key operations offline (e.g., when it is idle), and only does the online computation when the message to be sent is ready. Interestingly, we find that by allowing both RSA and ElGamal type systems in our scheme, we are able to reduce the computation cost compared with the pure ElGamal scheme proposed in [8]. This may look counterintuitive since it is known that the ElGamal system (implemented using Elliptic Curve Cryptography, or ECC for short) is much faster than the RSA system. The reason of this counterintuitive fact is that in our hybrid scheme, for most of the RSA nodes, we only need to do RSA signature verification, which is very fast since the RSA public exponent e can be very small. The proposed new SAMA scheme is compared with the previous scheme in terms of its execution time during signature generation and verification. We also implement our scheme in a laptop and in a Raspberry Pi to demonstrate its practicality.

ADVANTAGES OF PROPOSED SYSTEM :

1) High accuracy
2)High efficiency
3) Authenticity: The receiver and each forwarder in the routing path can verify that the message is sent by a legitimate data source, which can be a specific node, or a node in a particular group.
4) Integrity: The receiver and each forwarder in the routing path can verify that the message has not been altered during transmission.
5) Identity and location privacy: the identity and location of the message sender is well-protected. As mentioned before, the identity and location of a node may disclose some information about the data sent by that node.

SYSTEM REQUIREMENTS

- **HARDWARE & SOFTWARE REQUIREMENTS:**

➢ **HARDWARE REQUIRMENTS :**

- System : Pentium IV 2.4 GHz.
- Hard Disk : 40 GB.
- Ram : 512 MB.

➢ **SOFTWARE REQUIRMENTS :**

- Technology : Java 2 Standard Edition, JDBC
- WebServer: Tomcat 7.0
- Client Side Technologies : HTML, CSS, JavaScript
- Server Side Technologies : Servlets, JSP
- Data Base Server : MySQL
- Editor : Netbeans 8.1
- Operating System : Microsoft Windows, Linux or Mac any version

IV. IMPLEMENTATION:

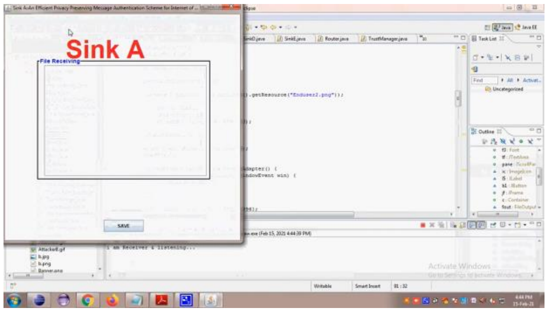
MODULES:

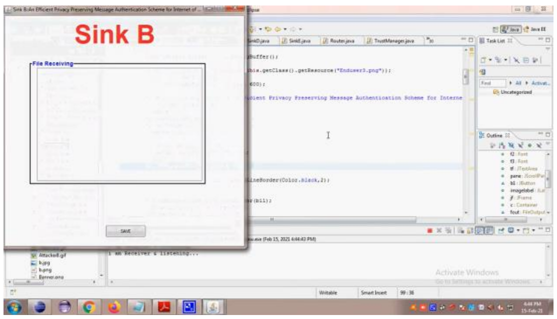
Upload currency image : use this button to get upload an currency image.

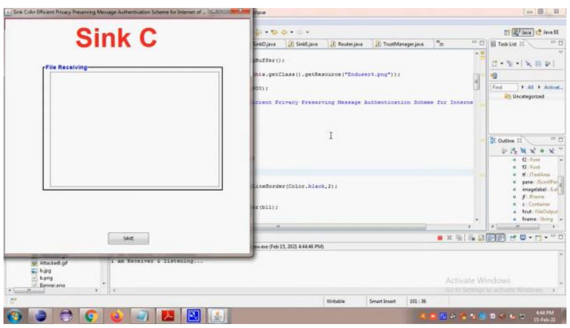
Run template matching currency recognition : use this module to get Run template matching currency recognition.

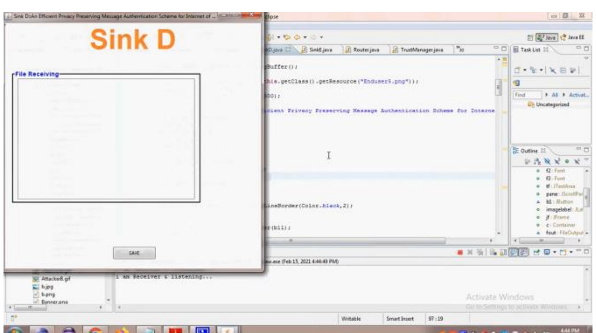
V. SCREEN SHORTS :

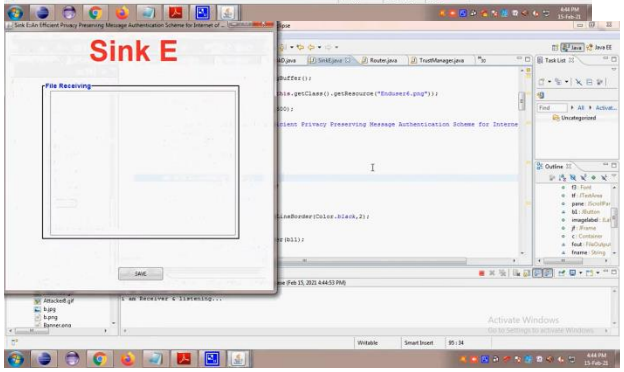
eISSN1303-5150

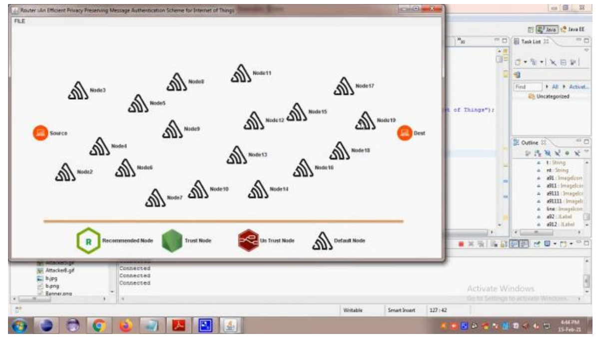

Sink A
File Receiving

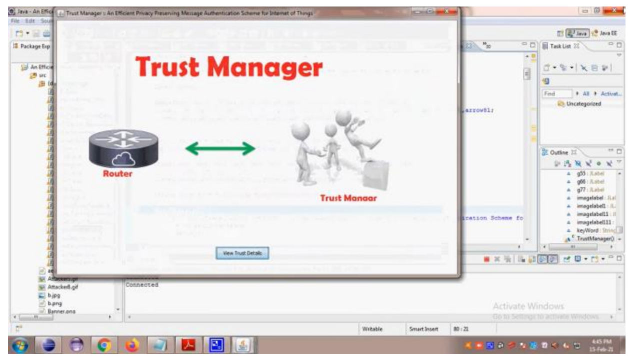

Sink B
File Receiving

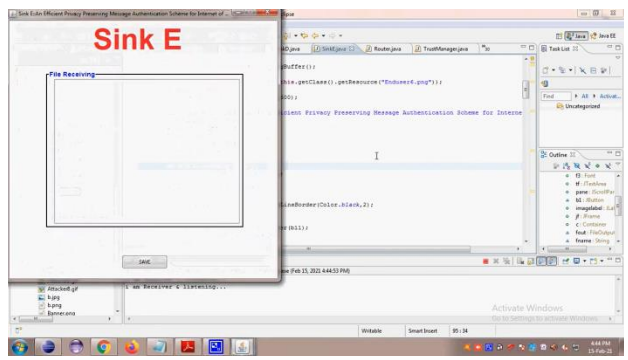

Sink C
File Receiving

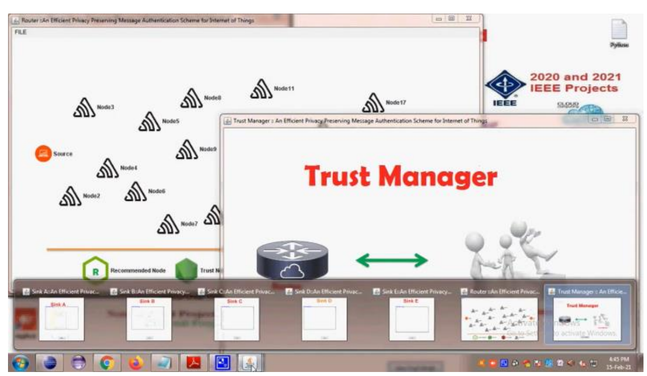

Sink D
File Receiving

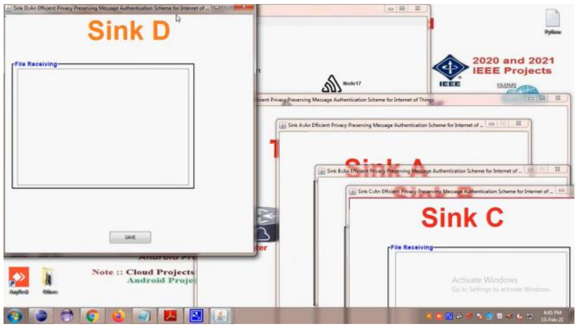

Sink E
File Receiving

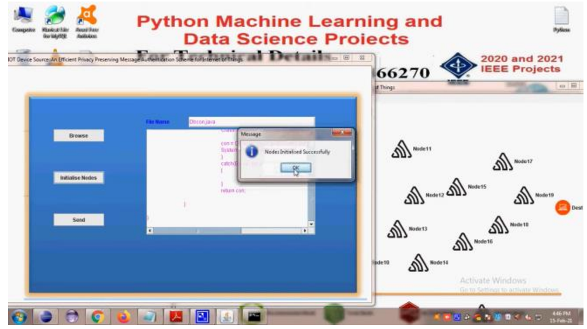


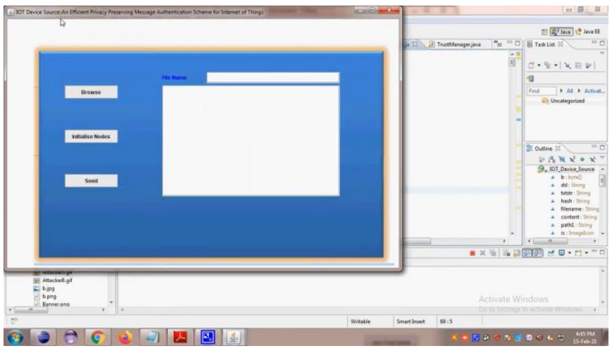

Trust Manager
Router
Trust Manager

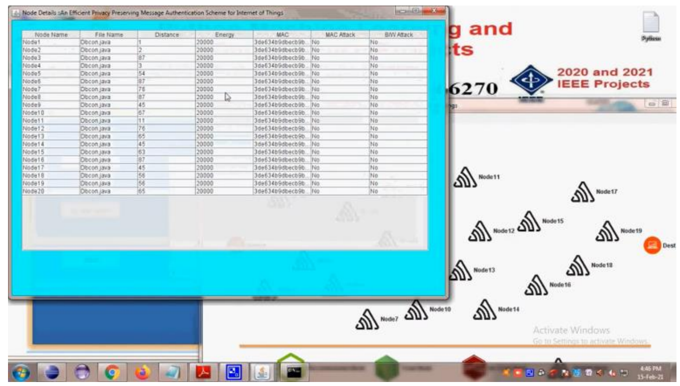

Sink E
File Receiving

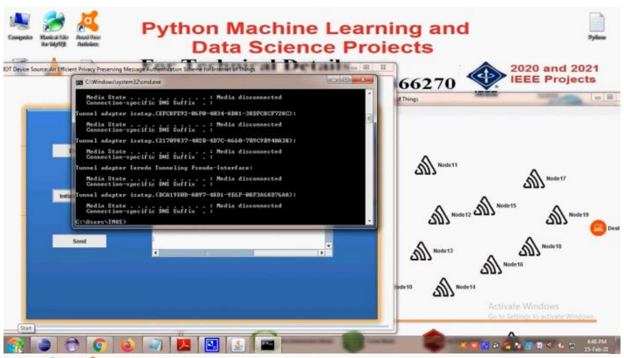

2020 and 2021
IEEE Projects
Trust Manager

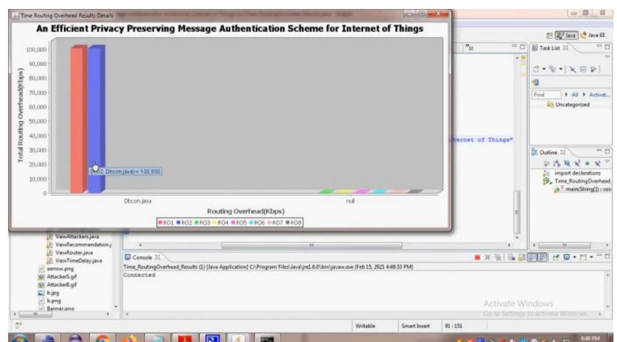

Sink D
Sink C
2020 and 2021 IEEE Projects

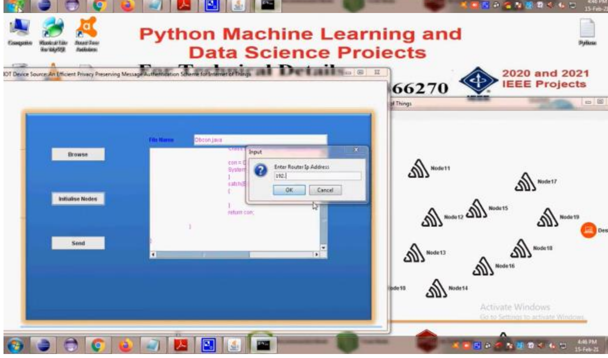

Python Machine Learning and Data Science Projects
2020 and 2021 IEEE Projects

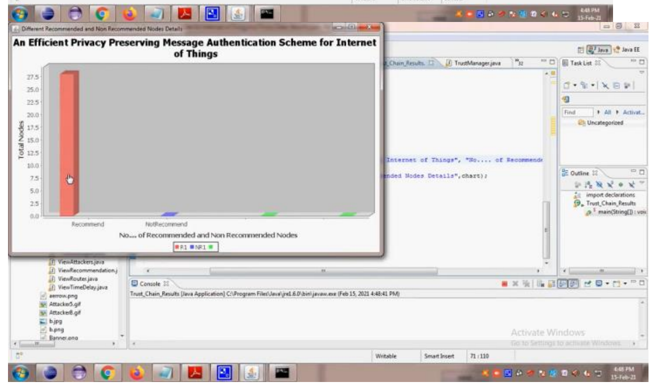


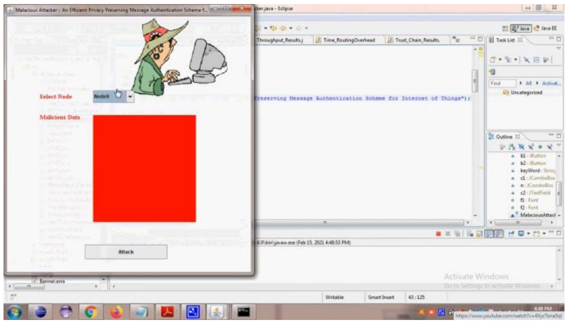

2020 and 2021 IEEE Projects

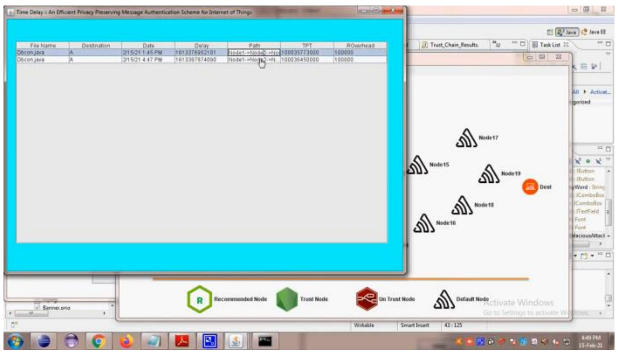

Python Machine Learning and Data Science Projects
2020 and 2021 IEEE Projects

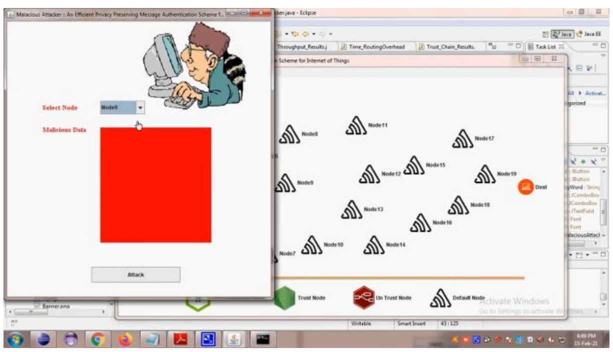

An Efficient Privacy Preserving Message Authentication Scheme for Internet of Things


Python Machine Learning and Data Science Projects
2020 and 2021 IEEE Projects


An Efficient Privacy Preserving Message Authentication Scheme for Internet of Things







VI. CONCLUSION :

We reexamined a privacy-preserving message authentication technique and demonstrated a security flaw in it in this research. In addition, we offered a workaround for the issue that eliminated any overhead. We have also presented a novel privacy-preserving message authentication scheme that enables IoT devices to use alternative security systems and parameters, providing greater practicality in an Internet of things that consists of several smart device kinds. Additionally, we used the offline/online computation technique to increase the suggested scheme's scalability and efficiency, making it more feasible than the earlier option.

REFERENCES

1] L. Da Xu, W. He, and S. Li, “Internet ofthings in industries: A survey,” IEEE Transactions on industrial informatics, vol. 10, no. 4, pp. 2233–2243, 2014.

[2] T. Song, R. Li, B. Mei, J. Yu, X. Xing, and X. Cheng, “A privacy preserving communication protocol for iot applications in smart homes,” IEEE Internet of Things Journal, vol. 4, no. 6, pp. 1844–1852, 2017.

[3] W. He, G. Yan, and L. Da Xu, “Developing vehicular data cloud services in the iot environment,” IEEE Transactions on Industrial Informatics, vol. 10, no. 2, pp. 1587–1595, 2014.

[4] J. Wei, X. Wang, N. Li, G. Yang, and Y. Mu, “A privacy-preserving fog computing framework for vehicular crowdsensing networks,” IEEE Access, vol. 6, pp. 43 776–43 784, 2018.

[5] M. Mohammadi, A. Al-Fuqaha, S. Sorour, and M. Guizani, “Deep learning for iot big data and streaming analytics: A survey,” IEEE Communications Surveys Tutorials, vol. 20, no. 4, pp. 2923–2960, 2018.

[6] J. Shen, T. Zhou, X. Liu, and Y.-C. Chang, “A novel latin-squarebased secret sharing for m2m communications,” IEEE Transactions on Industrial Informatics, vol. 14, no. 8, pp. 3659– 3668, 2018.

[7] P. McDaniel, N. Papernot, and Z. B. Celik, “Machine learning in adversarial settings,” IEEE Security Privacy, vol. 14, no. 3, pp. 68–72, 2016.

[8] J. Li, Y. Li, J. Ren, and J. Wu, “Hop-by-hop message authentication and source privacy in wireless sensor networks,” Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 5, pp. 1223–1232, 2014.

[9] T. ElGamal, “A public key cryptosystem and a signature scheme based on discrete logarithms,” in Advances in Cryptology - CRYPTO ’84, 1985, pp. 10–18

[10] D. Pointcheval and J. Stern, “Security proofs for signature schemes,” in Advances in Cryptology - EUROCRYPT ’96, 1996, pp. 387–398.

[11] R. L. Rivest, A. Shamir, and L. M. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” Commun. ACM, vol. 21, no. 2, pp. 120–126, 1978