Mirza Anas Beg,2021, 9:4
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

A Review on ANN Based Efficient and Secure Authentication Key Agreement Protocol for WSN In IoT

M. Tech. Scholar Mirza Anas Beg, Prof. Zuber Farooqui
Department of Computer Science and Engineering
All Saints' College of Technology, Bhopal, MP,India

Abstract-Data security plays a central role in the design of Internet of Things (IoT). Since most of the "things" in IoT are embedded computing devices it is appropriate to talk about cryptography in embedded systems. These kinds of devices are based on microcontrollers, which have limited resources (processing power, memory, storage, and energy). Therefore, we can apply only lightweight cryptography. The goal of this work is to find the optimal cryptographic solution for IoT devices. It is expected that perception of this solution would be useful for implementation on "limited" devices. In this study, we investigate which lightweight algorithm is better to implement. Also, how we can combine two different algorithms in a hybrid scheme and modify this scheme as per data sending scenario. This paper is focusing on a survey on IoT security and aims to highlight the most significant problems related to safety and security in the IoT ecosystems. This survey identifies the general threat and attack vectors against IoT devices while highlighting the flaws and weak points that can lead to breaching the security. Furthermore, this paper presents solutions for remediation of the compromised security, as well as methods for risk mitigation, with prevention and improvement suggestions.

Keywords: ANN, Secure authentication, IOT, Protocol, WSN

I. INTRODUCTION

The lack of trust in the digital world spurs from the use of online credentials with low levels of authentication assurance. Secure authentication is crucial for IoT systems given the fact that IoT devices may be deployed out in the open and remote locations.

This exposes them to physical attacks which was not a concern in the traditional Internet where personal computers are considered physically protected. Furthermore, the resource constrained nature of IoT devices makes the task of designing secure protocols even more challenging. In this paper we use Physically Unclonable Functions (PUFs) to establish the root of trust in IoT systems for authentication.

PUFs can provide a challenge-response mechanism by exploiting the (sub-) microscoping structure of integrated circuits. The use of PUFs can provide security against physical and cloning attacks [2].

Data provenance institutes trust in the origin and creation process of data. Through data provenance, a user can warrant confidence in the fidelity of data, i.e., that the data is indeed collected by the specific IoT device at the stated location and time. Trustworthiness of the data generated by IoT devices is of utmost importance for the correct operation of IoT based systems [3].

For example, consider the case of a nuclear power plant where the temperature and pressure need to be monitored and maintained within a strict range by IoT devices.

An adversary may try to invalidate this data by moving an IoT device to a different location or even cloning it.

1. Development of WSN towards IOT:
The Internet of Things consists of a variety of devices, or IP addresses assigned to these devices connected to a global network via the Internet.

Different IoT applications, such as healthcare and agricultural functions, can be deployed based on the requirement that wireless networks (WSNs) connect to real-time devices. This IP forwarding node transfers information to the central node, which does all storage or organizes large sensor data.

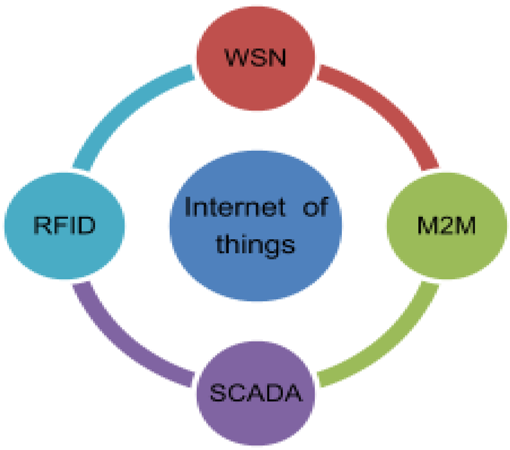

Fig 1. Role of WSN in IoT.

It is accomplished through a dedicated gateway, which is also answerable for flow of data among devices in the IoT world. Though, when we connect WSNs to the IoT, we will face a variety of challenges, including issues of security, application quality and application management.

2. Security Threats in Different Layers of IOT:

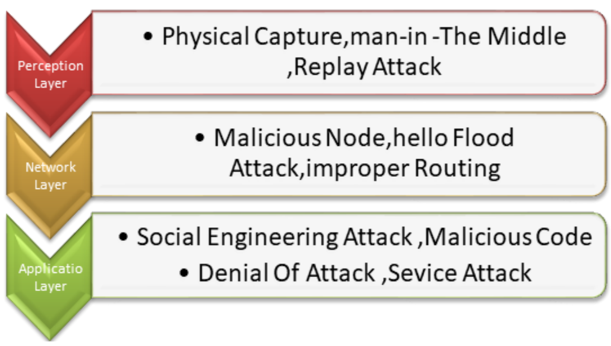

Fig 2. Attacks in Different Layers of IoT.

A protection threat is an act where it leverages safety limitation of an arrangement or produces a negative outcome on it by degrading the eminence of service of organization [4].Various probable attacks in unusual layers of IoT can be represented in figure 2.

II.LITERATURE REVIEW

We are current investigate work of some of the important authors in this field, giving a short description of different method used by them:

Muhammad Naveed Aman et.al.2019[1] The Internet of Things (IoT) engulfs a large number of interconnected heterogeneous devices from a wide range of pervasive application areas including health-care systems, energy management, environmental monitoring, and home and commercial automation. Although IoT is considered an enabling technology for a variety of services, it also raises many security and privacy concerns.

This paper focuses on developing secure protocols for data provenance with authentication and privacy preservation in IoT systems. Protocols for two scenarios are presented, one when an IoT device is directly connected to a wireless gateway and the other when an IoT device is indirectly connected to the wireless gateway through multiple hops of other IoT devices.

The proposed protocols use Physically Unclonable Functions along with wireless link fingerprints derived from the wireless channel characteristics between two communicating entities. This results in protocols which are not only efficient in terms of computational complexity and energy requirements but are also safe against various types of attacks including physical and cloning attacks.

Experimental results show that in comparison to existing protocols, the proposed protocols are upto 100% more accurate in detecting attacks on data provenance and can save upto 83.8% and 73.5% energy consumption for the IoT devices in terms of CPU and radio energy, respectively

In 2020 HakjunLeeaet al. [1] the authors proposed the user authentication schemes and proposed an updated method to correct and enhance the protection. A random Oracle, BAN logic, methods were used for formal and informal security analyses for security of the proposed scheme to be tested. The results of study show that the proposed system is safe, can withstand a large number of known attacks, and comply with all safety criteria.

Also, the Author conducts a benchmarking study based on the hardware features of mobile devices and sensors and other related solutions in the real world of the Internet of Things. The findings of the study show the compatibility of the solution with very low-cost IoT products. The approach planned in this study is therefore useful for IoT user authentication.

Sajid Hussein et. al. 2021 Continuous innovation and advancement of information, software and communication technologies will contribute to the rapid expansion and growth of Internet-of-Things (IoD) drone networks used by devices, applications and people to transmit and share data.

IoD can improve comfort in many applications, including everyday life in cities, businesses, and military / rescue operations. However, this increase in infrastructure visibility is also affected by new security threats, and resistance requires new solutions tailored to IoD. Several projects have been proposed recently to protect the IoD environment; however, some of them have proven to be unreliable, while others have reduced their effectiveness.

In this article, we use cryptography with an elliptic curve to present a new authentication plan to ensure the security of communication between the user and the drone flying in a specific flight area. The security of the proposed project was requested using the traditional oracle official method, and the security aspects provided by the proposed plan were briefly discussed. Finally, it explains the comparison between related and final programs.

Shahriar Ebrahimi; et. al.2021 and biometric technology devices have proven to be a reliable source of information, especially for Internet of Things (IoT) applications. One of the methods to use biometric data for identity verification is the Fuzzy Extractor (FE), which can extract secure and retrievable keys obtained from noisy biometric sources with no loss. It has been shown that FE can be reliably stabilized depending on the problem of the soft-sound similarity test (LPN), and the fault tolerance is higher than the previous FE plan. However, F-L-based applications in existing LPNs are only affected by excessive resource requirements, which are not suitable for IoT devices. This paper offers a lightweight hardware / software (HW / SW) co-design for the implementation of FE-based LPN.

We offer various architectural improvements to reduce program requirements. Compared to the previous work, the proposed design can withstand simple channel analysis and increase the area and area (AT) area by more than 89% and 83%, respectively. Our experimental results show that the proposed architecture can be applied to SoC-FPGA boards sourced from different vendors (such as Xilinx, Digilent, and Trenz). In addition, we use HW / SW co-design to provide the first solution of the ASIC-based LPN.

Braeken et. al. (2020) introduced a first method in this chapter. These methods use limited symmetric - based mechanics of hashing, XOR, and encryption / decryption to provide high latency and authentication. Based on ideas from a multi-server authentication platform, which has been applied to multiple IoT scenarios, it offers a comprehensive management protocol for wireless communication networks with a hierarchical structure that only works. -asymmetric based on fundamentally based education. The protocol establishes confidentiality, integrity and verification of identity.

It supports a variety of communication strategies, has limited storage requirements, is efficient at high energy by reducing the number of communication processes and processing encryption, and avoids the spread of messages accordingly chest.

By pre-installing separate keys between the base nodes and using other key tools at the cluster head and the cluster node, all keys in the network can be counted. and updated effectively in real time. We will consider the differences from the popular LEAP key management system for wireless sensor networks.

Zeeshan Ali et al. (2020) are able to use a variety of three-card-based solutions, which are designed specifically for remote medical information systems and can be used to authenticate remote users. In general, most of the existing solutions for TMIS are offered for both single -server environments and single -server environments. Therefore, patients are required to register and log in separately from each server to use different services, which will increase card retention and password storage for users. In a multi-server environment, users only need to register once to use various services to take advantage of the multi-server environment.

Recently, Barman et al. By fulfilling vague promises, the electronic health care verification project is proposed, and it is confirmed that the strategy can withstand many known attacks. However, after careful consideration, this article still points out the shortcomings associated with its design. In addition, the strategy of Barman et al. It is vulnerable to a number of attacks, including: server simulations, session key violations, user impersonation, covert attacks with secret parameter leaks, and anonymity. hidden by the user.

In addition, their project has measurement problems. To alleviate the above problems, this work provides a three-part infrastructure-based security enhancement proposal and a core protocol framework for multi-server environments (ITSSAKA-MS).

The safety of the ITSSAKA-MS was officially verified with the AVISPA automatic device, and the safeguards were discussed. However, the proposed strategy requires additional communication and calculation costs. In contrast, there is a form of informal and automated analysis that shows that, compared to the most recent measurement strategy, only the proposed strategy withstands many known attacks.

Timothy Malcheet.al(2020) Internet of Things (IoT) security requires the security of connected objects and networks. The Internet of Things is increasingly a collection of so -called unique objects. These objects have the ability to send data automatically through the network.

Most of the growth of IoT connectivity comes from computing devices and integrated metering systems that are used for machine-to-machine (M2M) communication, home automation and home automation in-vehicle communication, sharp gridsand usable tools. Since it is to connect all physical objects to the Internet, the idea is not always evaluated in product design.

IoT products cannot choose secure security. Therefore, security is one of the most important priorities in the Internet of Things. This research proposes an IoT architecture that is related to device security. The main purpose of this research is to ensure that the real device uploads the data and limits the fake data generated by the device trying to become a real device. This research offers a powerful authentication technology based on secret keys that can protect the identity of IoT devices in a network.

The authentication and authentication technologies presented in this article can ensure that the right equipment transmits and receives the right data at the right location and for the right purpose.

III.RESEARCH MOTIVATION

The Internet of Things is a constantly evolving knowledge that can connect multiple devices to remote services via the Internet. Because of the capabilities of the tools included, it is important to distribute resources from third-party platforms. A lot of research is underway to connect IoT devices to multiple resource pools.

Some of these aspects include the basics of mathematics, protocol design, curve design, security proofs, point substitution, natural arithmetic algorithms in algebraic structures, application strategies in software, tools and attack models.

The main advantage of lightweight authentication is that, compared to other cryptosystems, shorter keys can be used (memory required and faster local arithmetic work), which makes it a more controllable tool. resources (For example, it is suitable for implementing basic public cryptography on devices. Applications that can be found in expected applications for the Internet of Things.

The Internet of Things (IoT) paradigm has become more significant. The main components of Internet of Things are RFID, sensors or actuators, which are moderately small in size or low in power consumption.
The different settings with IoT approach include wireless sensor complex or wireless low-power zone networks. Since wireless sensor networks are easy to put into application in a very large number of times, the area of concern is wireless sensor networks.

In addition to scalability and mobility of wireless sensor networks for a variety of harsh conditions, wireless sensor networks also have many points of interest. They also face a few issues, such as load and energy limits, and sensor channel attacks and other common attacks (e.g. simulation, replay attacks).

One of the security challenges identified among the major issues to be addressed is authentication within the network. In a sensor situation, if the network does not have authentication properties, it is fairly certain that the intruder can appear as a justifiable user and obtain basic information about the network [5]. Therefore, if there is a new exterior user or device ready to converse with other devices in the complex, it should be confirmed if it is a legal device.

All existing validation strategies developed for validation are very effective in one respect, but there are still limitations when using these schemes. Based on an analysis of their presentation, it can be assumed that sometimes these process will lead to the energy consumption of the sensor equipment and also bring some computational overhead toNetwork.

In order to conquer the effects of using composite verification procedures, it is suggested to choose a lightweight verification procedure to recover the concert of the sensor devices in organization.

IV.PROBLEM STATEMENT

Provides a common authentication solution that reduces the number of messages replaced during authentication procedure or makes it much simpler, which will use simple operations to reduce the resource expenditure of the network.

Basic authentication tools designed for resource-limited sensor networks, which is a core technology for IoT applications. Evaluate the protocol's resistance to active and passive attacks known in the Internet of Things sensory field. Evaluate various performance indicators, such as computational time, overhead of the relationship to the developed protocol, and compare with existing protocols. Existing symmetric algorithm solutions based on the secure lightweight authentication protocol to mitigate outcome of attack in the IoT network.

We use the elliptic curve insertion method, which provides the same protection for smaller key sizes, and compared to the symmetric system (AES) used together to generate a key that is used to reduce the accuracy of the device at registration, name and verification.

The man-in-the-middle attack usedfor efficient analysis of system and a back propagation neural network for supervised learning to optimize the IoT network to reduce overhead consumption and attack detect.

V.CONCLUSION

This paper offers market-available solutions to deal with the lack of identity, access, and trust for IoT products and services; proposes new data-computing models to address the scalability, complexity, and management of the environment; and elaborates on the concept of security by design to meet the requirements for device management.

Although this paper advises IoT makers to seek new ways and methods to adapt their offerings to the new ecosystem and move away from traditional IT security practices, more research is needed on the topic. The responsibility for implementing proper security solutions does not depend on a single party of the IoT ecosystem, but rather on all the actors involved, from silicon suppliers to manufacturers, to developers, to lawmakers, and the final customer.

Mitigating risks associated with security breaches are possible, if security receives consideration from early product planning and design, and if some basic prevention mechanisms are in place.

Enactment and standardization will simplify the manufacturing and development processes, give the market an incentive for mass- adoption, and also increase the security posture of IoT products and services. Security will have to be inbuilt so that IoT can withstand a chance against the threats that technology advancements will bring along.

REFERENCE

[1] HakjunLeea, Dongwoo Kanga, JihyeonRyub, DonghoWonc, HyoungshickKimc, Youngsook Lee "A three-factor anonymous user

authentication scheme for Internet of Things environments" ELSEVIER 2020.

[2] Anca Jurcut, TiberiuNiculcea, PasikaRanaweera, Nhien- An Le- Khac "Security Considerations for Internet of Things: A Survey" SN Computer Science 2020.

[3] Chi-Tung Chen, Cheng-Chi LeeID, Iuon-Chang Li "Efficient and secure three-party mutual authentication key agreement protocol for WSNs in IoT environments" PLOSE ONE 2020.

[4] Liang Xiao, He Xu, Feng Zhu, Ruchuan Wang, and Peng Li "SKINNY-Based RFID Lightweight Authentication Protocol" MDPI 2020.

[5] Evangelina Lara, Leocundo Aguilar, Mauricio A. Sanchez, and Jesús A. García "Lightweight Authentication Protocol for M2M Communications of Resource-Constrained Devices in Industrial Internet of Things"MDPI 2020.

[6] AfrahAlbalawi, Amal Almrshed, Arwa Badhib, SuhairAlshehri "A Survey on Authentication Techniques for the Internet of Things" IEEE 2019.

[7] Seul-Ki Choi, Ju-Seong Ko, Jin Kwak "A Study on IoT Device Authentication Protocol for High Speed and Lightweight" IEEE 2019.

[8] Zaheer Abbas, Syed Muhammad Sajjad, Hassan Jalil Hadi "Light Weight Secure Authentication for Accessing IoT Application Resources" IEEE 2019.

[9] Mohammed El-hajj, Ahmad Fadlallah, Maroun Chamoun, and Ahmed Serhrouchni "A Survey of Internet of Things (IoT) Authentication Schemes" MDPI 2019.

[10] Feng Zhu, Peng Li, He Xu, and Ruchuan Wang "A Lightweight RFID Mutual Authentication Protocol with PUF" MDPI 2019.

[11] Akber Ali Khan, Vinod Kumar, Musheer Ahmad "An elliptic curve cryptography based mutual authentication scheme for smart grid communications using biometric approach" Journal of King Saud University 2019.

[12] Feifei Wang, Guoai Xu, and Lize Gu "A Secure and Efficient ECC-Based Anonymous Authentication Protocol" Hindawi 2019.

[13] SungJin Yu, KiSung Park, and YoungHo Park "A Secure Lightweight Three-Factor Authentication Scheme for IoT in Cloud Computing Environment" MDPI 2019.

[14] Valmiki Siddhartha, Gurjot Singh Gaba, Lavish Kansal "A Lightweight Authentication Protocol using Implicit Certificates for Securing IoT Systems" ELSEVIER 2019.

[15] Data Provenance for IoT with Light Weight Authentication and Privacy Preservation Muhammad Naveed Aman, Mohammed Haroon Basheer, Student Member, IEEE BiplabSikdar, Senior Member, IEEE 2327-4662 (c) 2019 IEEE.