International Journal of Scientific Research in Computer Science, Engineering and Information Technology

ISSN : 2456-3307 OPEN ACCESS

Available Online at : www.ijsrcseit.com

doi : https://doi.org/10.32628/CSEIT2390662

Enhancing Privacy and Security for Sensing Applications in Wireless Community Networks

Sumalatha Kulkarni*, Pradeep Nerupati, Lahari Ailineni

Information Systems, New Jersey Institute of Technology, Newark, New Jersey, United

ARTICLEINFO

Article History:

Accepted: 10 Dec 2023

Published: 27 Dec 2023

Publication Issue

Volume 9, Issue 6

November-December-2023

Page Number

310-315

ABSTRACT

Wireless Community Networks (WCNs) have become a viable option for underprivileged areas to have internet access. These networks are fundamentally open and decentralized since they are created by a community of users who contribute resources like bandwidth. The open architecture of WCNs and decentralized nature, and not having well defined regulation policies in place, necessitate addressing privacy and security issues around WCNs. Especially for sensing devices / applications that transmit large volumes of data, having strong security and privacy measures becomes essential. We are basing our research on the invited paper by Delphine et al., (2010) for taking the proposed solutions further [1].

Keywords : WCNs, Sensing Devices, Security and Privacy, Encryption

I. INTRODUCTION

Wireless Community Networks: Simply put are networks put together by a group of people and for people. These networks first started emerging to provide internet connectivity to rural, underserved and geographically challenging areas by community-driven organizations or a community of people themselves (like in peer-to-peer networking) where the infrastructure is formed by pooling in the existing resources and partnering within the group/ community to start up and scale. They operate on the mesh networking principles. Being community-driven and collaborative, they are decentralized meaning they don't have a single point of failure. They operate in the unlicensed Wi-Fi spectrum of 2.4 GHz and 5 GHz, keeping the costs lower than costs charged by traditional ISPs. They are playing a major role in narrowing the digital divide between urban and rural areas providing broadband internet at low cost or no cost by volunteer organizations.

The WCN needs an internet source which is often a high- speed connection from an ISP that the WCN can tap into, which is then distributed across the WCN connections. This type of setup has a limitation that the connection from the ISP internet source have a direct line-of-sight and not have obstacles in the path. Obstacles in the path cause the connection to become weak due to interference and absorption. [4]

Champaign-Urbana Community Wireless Network [2]

II. HISTORY

Evolution, Need for WCNs WCNs started in around the late 1990s and early 2000s as open-source movements were catching on. They were set up as experiments by do-it-yourself enthusiasts, by a community of people to make internet connectivity accessible in rural and underserved areas.

There are a growing number of WCNs across the globe. NYC Mesh (NYC), Ninux.org (Italy), Wireless for Communities (W4C, an award-winning initiative by the Internet Society Asia Pacific Bureau for remote areas in Asia-Pacific rural and remote areas) are some of the examples of WCNs. WCNs have been built in emergency situations for providing essential communications over the wireless network. Wireless Community Network technicians Paul Smith and Rogers Wilson III, set up wireless links with the help of local volunteers to local hospitals and emergency services during Katrina. [5], [6]

NYC Mesh 'supernode' in Manhattan [3]

There are many reasons why WCNs may be built other than serving the underserved / unserved areas. People who want to democratize the internet, have open and affordable networks, help local communities grow economically and become more cohesive, want more autonomy over their networks and self- organization may come together to build one. Below is an example of NYC Mesh's super node (right in the urban settlement).

III.Open Issues and Challenges

The Internet is a complex place and has been changing dynamically since its origin. In recent years we have seen its rapid proliferation with newer protocols and technologies developed every day add to the complexities and challenges. All the data security issues during transit that plague Wi-Fi technology apply to WCNs.

Despite the many positive offerings of WCNs, however, the open nature of these networks presents significant privacy and security challenges. Unauthorized access, insecure communication protocols, data interception and tampering opportunities are a few to name. These privacy and security issues alongside the case that there are not particularly well defined legal or regulatory guidelines or laws, make it particularly important for addressing them. Especially when it comes to sensing applications within WCNs which may transmit personal data like health information, biometric information like iris scans, fingerprints, facial detection etc., the need to secure them becomes top priority.

James Stevens, co-founder of consume.net, also explains that users were warned: "We run an open wireless network. So, no passwords for access but encrypted tunnels between network nodes and internet gateways. If this is a concern or messages need security, then it's the responsibility of everyone to guard against intrusion and practice effective methods. Those who wish to communicate in secret will always find a way of achieving this goal. Once through the gateway we have no control anyway."

"Sensor networks are becoming increasingly popular to provide economical solutions to many challenging problems such as real-time traffic monitoring, wildfire tracking, wildlife monitoring, or building safety monitoring. In sensor networks, thousands of sensor nodes collectively monitor an area. These large sensor networks generate a substantial amount of data, yet the sensor nodes often have limited resources, such as computation power, memory, storage, communication, and most importantly, battery energy. The large scale of sensor rce constraints make it an important and develop efficient information tion techniques to make effective use query, it may be unnecessary and raw data collected from each sensor— hould be processed and aggregated nd only processed and aggregated In such a setting, certain nodes in the ed aggregators, collect the raw nsors, process it locally, and reply to a remote user. However, information r networks is made even more that the sensor nodes and aggregators ronments may be compromised due to ng and aggregation mechanisms need to be resilient against attacks where the aggregator and a fraction of the sensor nodes may be compromised." [7]

In our research, we delve into the world of zero-knowledge proofs, homomorphic encryption, and their real-world applications in enhancing privacy and security for sensing applications within WCNs.

IV. Design Discussion

A. Data Protection for Home Security Devices:

Home security devices will capture sensitive environmental data around the household. This data could be environmental sensor data such as humidity, security camera footage, glucose, and cholesterol level data from vital sensors.

We looked at homomorphic encryption techniques for the goal of securing sensor data. The goal of homomorphic encryption is to allow gathering insights by analyzing this data without compromising security and privacy.

Cloud-based analytic tools that make use of encrypted data can be advantageous to homeowners. This makes it possible to respond to possible security threats with alerts or notifications in real-time. The homeowners' privacy is protected by homomorphic encryption, which inhibits illegal access to unprocessed video and environmental data. Algorithms for anomaly detection, for example, can spot odd activity without jeopardizing the integrity of the underlying data.

Homeowners have control over the decryption procedure while using homomorphic encryption. When necessary, they can selectively decrypt and retrieve data, allowing them to examine video recordings or verify past environmental conditions. This guarantees that homeowners retain control over important personal information.

B. Homomorphic Encryption:

Unlike other encryption techniques, homomorphic encryption allows mathematical operations to be carried out directly on the encrypted data, potentially improving the security of third- party handling of user data. It could be difficult for businesses to adhere to compliance requirements to safely outsource data to a third-party environment for processing, analytics, or storage. However, homomorphic encryption eliminates the need to rely on a third party's data security when outsourcing data processing or analytics. We have seen machine learning as a service (MLaaS) evolve in recent years. Typically, the users would provide their input to the service provider, who would then run some algorithms over the information and return the outcome. Because they are concerned about their privacy, consumers might not want to give their data to the service provider.

In the context of cloud computing, homomorphic encryption may be crucial since it allows businesses to keep encrypted data on public clouds and utilize the analytics capabilities offered by the cloud provider.

C. Zero-knowledge proofs

Zero-knowledge proof is a security feature in blockchain technology that makes credential validation easier without disclosing the real credentials. ZKPs make it possible to verify computations without transferring raw data. As a result, communication is more effective, and less data is sent across the network.

Zero-knowledge proofs enable a prover to establish a statement's validity without disclosing any further details about the statement. This is accomplished by offering proof, or a tiny quantity of data, that may be checked by a verifier to confirm the integrity of the statement.

In the financial sector, for instance, a client might wish to verify their identification with a bank without disclosing any personal information, such as their social security number. The bank is the verifier in this case, while the customer is the prover. The customer gives the bank identification that can be used to confirm their identity, like a government-issued ID.

The bank may then verify, without disclosing any private information, that the client is who they say they are.

Vulnerabilities include weak cryptography, repudiable transactions, single points of failure (SPOF), inadequate access restrictions, and weak cryptography. Zero-knowledge proofs and blockchain technology can help minimize the risk of Man-in-the-Middle (MiTM) and supply chain attacks in B2B healthcare electronic data interchange. The vulnerabilities range in severity from major to minor. [8], [9], [10]

V. Methodology

In this our research endeavour, we have simulated a home security system, integrating HE and ZKP technologies to fortify the premises security and ensure a robust access control mechanism. The primary objective of this study is to establish a seamless and secure interaction between a security camera and a server, employing advanced techniques such as zero-knowledge proofs and homomorphic encryption.

```
from lightspeed import LightPHE

#client side code showing Homomorphic Encryption
cryptosystem = LightPHE('Paillier')
data1 = 10 data2 = 20
encryptedData1 = cryptosystem.encrypt(data1)
encryptedData2 = cryptosystem.encrypt(data2)
#server side operation showing Homomorphic Encryption encryptedSum = encryptedData1 + encryptedData2
```

The central point in our design is a home security camera that initiates a face recognition program on the server for determining whether an individual should be granted access to the premises or denied entry by the homeowners. But, to establish a trustworthy connection, registration of the security camera device with the server is a prerequisite. This registration process is a critical step in ensuring the security, identity, and location privacy of the device. To achieve this, we employ the zero-knowledge proof [ZKP] technique, allowing the security camera to prove its identity without disclosing sensitive information.

During the registration process, a tensor from a person's (homeowner's) photo is generated, which is a unique representation of the individual, and is encrypted, using homomorphic encryption. This is stored in the server for subsequent comparisons in the face recognition events. Homomorphic encryption ensures that the tensor remains confidential even during transmission to the server, thereby preventing any potential interception or compromise of sensitive data.

```
#client side code converting photo to tensor total = cs.decrypt(encryptedSum)
picam = PiCamera()
```

```
picam.capture("/home/pi/Pictures/photo.jpg")
capturedPhoto =
Image.open("/home/pi/Pictures/photo.jpg")
sourceTensor = transforms.ToTensor()
sourceTensor(capturedPhoto)
```

When the security camera captures footage, it again generates a tensor (which is unique again) representing the person in the footage. This tensor undergoes homomorphic encryption before being transmitted to the server, just like during the registration process. The server's face recognition algorithm calculates the encrypted squared Euclidean distance between the tensor derived from the original photo and the tensor extracted from the footage.

tensor1 = (x1, y1, z1)
tensor2 = (x2, y2, z2)
SquaredEuclideanDistance = (x1 − x2)2 + (y1 − y2)2 + (z1 − z2)2

Most importantly, this computation occurs entirely in the encrypted domain, preserving the privacy and integrity of both tensors. The server, without decrypting the tensors, returns the encrypted result to the client. The onus then falls on the client to decrypt the squared Euclidean distance and make an informed decision on whether to allow or disallow the person based on it. If the calculated squared Euclidean distance is less than 100, then the compared tensors are of the same person and hence can be allowed entry or access, otherwise deny entry or access.

This integrated approach, which uses zero-knowledge proofs & homomorphic encryption in combination makes face recognition more secure, establishing a robust and privacy- centric home security framework. By ensuring that sensitive data remains confidential throughout the entire process, our methodology stands as a testament to the fusion of these latest technologies for safeguarding homes while safeguarding individual privacy. As the landscape of security challenges keeps becoming complex every day, we believe our study is a paradigm that prioritizes both technological innovation and ethical considerations in the domain of smart home security.

II. Conclusion:

Zero Knowledge Proof evolved from a theoretical concept to practical solution for secure data verification. It has been around since 1989 and is extensively used in blockchain technologies due to the transparent nature of distributed ledger concept. Its long time standing speaks for itself and its success. Incorporating ZKPs into our design of smart home security in the context of WCN where there are no standardizations of security protocols for access is a step in the right direction.

Homomorphic Encryption is a public key cryptography technique that allows calculations to be performed on encrypted data. Homomorphic Encryption, as a concept, was first introduced in 1978 by Rivest Adleman and Dertouzos. In

2009, a major breakthough occurred when Craig Gentry, a Stanford University PhD student constructed the first fully homomorphic encryption scheme as part of his dissertation. Since then, Homomorphic Encryption has been around, but the widespread practical application is still limited due to challenges like computational efficiency and complexity.

In our design, we used the homomorphic TenSEAL library for a facial recognition use-case. Thus, facial embeddings can be kept in the cloud system without causing privacy issues. This again is a definite step ahead in securing sensing devices and applications within WCNs. We faced challenges due to the limited computational capacity available on our machines.

VI. CONCLUSION

Our conclusion is that Homomorphic Encryption is an area where practical application is still being explored. In the context of WCNs, application of Homomorphic Encryption for facial recognition may not be a practical solution as WCNs are built by a group of people who come together and contribute resources and those resources may not be robust enough or have high computational capacities. Practical application of Homomorphic Encryption is an active area of research. Hence, we conclude that this is an area that can be further explored.

VII. REFERENCES

[1]. https://ieeexplore.ieee.org/abstract/document/5560129
[2]. Champaign-Urbana Community Wireless Network https://cnt.org/sites/default/files/publications/CNT_Com munityWirelessNetworks.pdf
[3]. https://www.cbc.ca/news/science/wifi-nyc-mesh-new- york-city-1.4617106
[4]. https://www.netcommons.eu/sites/default/files/telecom- reclaimed-web-single-page.pdf
[5]. https://www.intgovforum.org/en/filedepot_download/4391/2376
[6]. https://cnt.org/sites/default/files/publications/CNT_Com munityWirelessNetworks.pdf
[7]. SIA: Secure Information Aggregation in Sensor Networks https://dl.acm.org/doi/10.1145/958491.958521
[8]. https://www.tandfonline.com/doi/full/10.1080/25765299.2023.2188701
[9]. https://ieeexplore.ieee.org/document/9252935
[10].https://people.csail.mit.edu/silvio/Selected%20Scientific %20Papers/Proof%20Systems/The_Knowledge_Compl exity_Of_Interactive_Proof_Systems.pdf

Cite this article as :

Sumalatha Kulkarni, Pradeep Nerupati, Lahari Ailineni, "Enhancing Privacy and Security for Sensing Applications in Wireless Community Networks ", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 9, Issue 6, pp.310-315, November-December-2023. Available at doi :
https://doi.org/10.32628/CSEIT2390662
Journal URL : https://ijsrcseit.com/CSEIT2390662