Smart Home Security: Leveraging Differential Privacy, SMPC, and Homomorphic Encryption.

Group 1

Mounika Sanaboyina,

Jaswanth Reddy Narala,

Ava Sharif Jourabchi,

Jaideep Naidu

University of Missouri Kansas City

CS 5533 Applied Cryptography

Sravya Chirandas

Fall - 2024

Contents

Abstract

The rise of smart homes leveraging the Internet of Things (IoT) has brought significant privacy and security concerns due to the vast amount of data exchanged between devices. This project addresses these challenges by employing differential privacy, secure multi-party computation (SMPC), and homomorphic encryption. These methods ensure that individual user data remains confidential, even when used for analysis and decision-making within the smart home ecosystem. Homomorphic encryption allows computations to be performed on encrypted data without decrypting it, further enhancing data security. This approach enables users to share their data confidently, without fear of misuse or compromise. The project aims to benefit consumers by safeguarding their data and providing developers of smart home systems with valuable insights. By integrating these advanced cryptographic techniques, the project not only enhances user trust but also promotes the broader adoption of smart home technologies. Additionally, it mitigates the risk of unauthorized access and data breaches, ensuring a safer smart home environment. Ultimately, this project represents a significant step forward in the secure and private development of IoT-enabled smart homes.

Keywords: Smart Homes, Differential Privacy, Multi-party Computation, Homomorphic Encryption, Privacy, Security, Cryptographic

Introduction

The Internet of Things (IoT) is evolving quickly, and the smart home concept has gotten a tremendous uplift over the last decade. The idea is to transform existing homes into linked, convenient, environmentally sustainable, and quality enhancing smart houses thus turning a new page in residential development. Consequently, many IOT devices such as the favourite voice assisted and heating coolers like smart thermometers are which used into this new Smart Home Era but also into our daily routines (Haseeb Touqeer, Shakir Zaman., 2021). The physical comparison systems have resulted in a significant era, marked by enhanced linkages and increase in the use of automatic devices. The Internet of things is the interconnection of physical products that are equipped with sensors, software's and other technologies thus making it easier for data to be collected, processed and disseminated through the use of automations. This translates to wearable technology, smart appliances, and security cameras working together to create a bright, networked house in the context of smart homes.

Although there are lots of advantages attached to IOT in new smart home technology, the main challenge it faces today comes from the users themselves. It is imperative to realize that the inclusion of smart devices in people's everyday life causes an increase in the amount of data flowing through these devices. However, the limits of that data may be too much in ways of their behavior, personality or the information of violence correlation, this can be a risk factor for people (Chunmao Wu,2022). It should be also understood that the smart home devices are monitoring every bit of the consumer's data today, and the data creation is volumetric and poses a risk, hence there is the question of securing privacy.

Emerging Discharge of Smart Home Systems

Although there are numerous benefits to a smart home, privacy and security are also issues. These systems also gather enormous amounts of data from various sources,

including private data that includes daily activities and personal preferences. This increases the likelihood that the data may be misused or used without authorization. Furthermore, every linked gadget in a smart home may give way to outside hackers who may use these flaws to gain access to the system.

Security:

An additional important concern with smart home systems is security. Hackers may gain access to devices within a home by compromising the hardware and software security. This suggests that a number of threats could materialize, including the capacity to remotely key in, control security systems and turn off alarms. Additionally, unprotected smart home appliances frequently join a botnet that lunches extensive cyberattacks.

The Project Objective issues in Addresses

This project uses Secure Multi-Party Computation (SMPC) and Differential Privacy, two essential cryptographic algorithms, to address privacy and security issues with smart home systems. A privacy technique called Differential Privacy introduces noise into quantitative data in order to protect personal information. Applying differential privacy to smart homes is essential to increasing their security since it ensures that the information gathered is not connected to specific individuals and cannot reveal their activities in detail. It lessens the likelihood that privacy will be breached and that personal information will be improperly disclosed.

Secure Multi-Party Computation does not reveal any individual input, but it does allow several entities to compute collectively over their personal data. SMPC in smart home systems allows us to make decisions and perform safe calculations without jeopardizing data privacy. Therefore, it implies that if someone has broken into the system, they won't be able to access important data or alter documents without everyone's consent.

It will be possible to ensure security and protect the privacy of the people living in this house by integrating these cryptographic protocols into a smart home system. They will be reassured that their personal data is secure, and the likelihood of unauthorized access and system manipulation will be decreased. Additionally, depending on these protocols lends credibility to smart home systems, making people more inclined to embrace them.

Problem Statement

As individuals look for convenience, home automation through smart home systems has been growing in popularity for some time. In addition to the requirement to gather private and sensitive data, the proliferation of connected devices has exacerbated security and privacy concerns. There are several security solutions available to address the issues with smart homes, such as authentication, which restricts access to those authorized by administrator. Multi-factor, biometric, and password-based authentication may aid in achieving this objective (Emanuela Marasco, 2023). Encryption is another crucial technique, in which data is transformed into a cipher that requires the original key to decrypt. Additionally, additional access control methods, such as attribute-based and role-based access control, limit user access to certain data or devices.

Data aggregations and anonymization are two strategies that make sure these systems don't use a person's information to identify them. Additionally, differential privacy adds random noise to the gathered data in order to preserve data that is sensitive to data protection. According to the principles of privacy by design, privacy should be considered from the beginning of a system with an eye toward end-user control, purpose limitation, and data minimization. But even with the increased efforts to protect smart home users' privacy and improve data security, problems still arise, which makes it necessary to create a more powerful security system that makes use of cryptographic methods.

Literature Review

Overview of SMPC and Differential Privacy Cryptography Protocols

Differential Privacy

Differential Privacy (DP) is a privacy-preserving technique that allows for the analysis of data containing sensitive information while ensuring individual privacy. The primary principle of DP involves adding noise to the data, which introduces randomness to protect individual contributions from identification. This added noise ensures that it becomes significantly harder to infer specific personal details based on the results, even when analyzing sensitive data. For example, DP can be applied in smart home environments to analyze energy consumption trends without revealing individual usage patterns, thereby protecting user privacy. This anonymization of data helps prevent disclosure of personal routines or habits that might compromise privacy.

Secure Multi-Party Computation (SMPC)

Secure Multi-Party Computation (SMPC) is a cryptographic approach enabling multiple parties to jointly calculate a function based on their private inputs without revealing those inputs to each other. This protocol supports secure collaboration and decision-making without relying on a trusted intermediary. Within the context of smart homes, SMPC could allow for secure access control determinations when multiple residents have varying levels of access. It achieves this by calculating decisions based on shared inputs without disclosing individual permissions, thus safeguarding data such as security codes or schedules from unauthorized exposure. SMPC relies on cryptographic techniques such as secret sharing and secure multiplications to keep computations private while only releasing results to authorized parties. Implementing SMPC in smart homes strengthens data protection and prevents vulnerabilities that could compromise residents' privacy.

Integrating Differential Privacy and SMPC in Smart Home Systems

Combining Differential Privacy and SMPC in smart home systems offers a robust framework for privacy and security. Differential Privacy ensures that aggregated data remains anonymous, preventing the disclosure of individual identities or private details . By adding noise to data, attackers are further deterred from extracting meaningful personal information. This strategy defends against unauthorized access to residents' sensitive data.

On the other hand, SMPC allows for secure computations without sharing specific inputs, enabling smart home systems to make informed decisions while protecting user privacy. For example, SMPC can be used to calculate collective energy usage in the household without exposing individual consumption data (Liu & Huang, 2021). Integrating these protocols requires designing secure cryptographic methods for data collection, storage, and analysis, as well as creating protocols for safe communication among devices involved in decision-making processes. Recent advances in DP and SMPC have led to effective algorithms and protocols that allow for practical privacy-preserving data analysis and secure collaboration, addressing privacy and security needs in smart home environments.

Encryption schemes and techniques play a pivotal role in securing data in Internet of Things (IoT) applications, where devices often handle sensitive information but operate in environments with limited resources. Given the constraints on processing power and storage capacity, the choice of encryption must balance strong security with efficiency. IoT encryption methods primarily include symmetric and asymmetric encryption, as well as advanced techniques like homomorphic encryption.

Symmetric Encryption is one of the most widely used techniques due to its computational efficiency. Algorithms such as Advanced Encryption Standard (AES) are commonly employed in IoT for tasks such as securing communication channels. However, the need to securely manage and distribute keys can be challenging, especially in networks with many nodes (Kumar et al., 2021). Asymmetric Encryption, on the other hand, allows for

secure key exchanges without requiring a pre-shared key. Algorithms like RSA and Elliptic Curve Cryptography (ECC) are favored, particularly ECC, as it requires smaller key sizes and provides similar security levels, making it ideal for IoT devices with limited processing power. However, asymmetric encryption tends to be computationally heavier than symmetric encryption.

Homomorphic Encryption (HE) represents a promising approach for IoT security. HE allows computations to be performed on encrypted data without needing decryption, making it ideal for privacy-preserving data processing on external servers or cloud services. This method is especially relevant for IoT, where devices often offload data to the cloud. Research shows that while fully homomorphic encryption is computationally intensive, partially homomorphic encryption schemes, like those allowing addition or multiplication, are feasible for specific IoT applications. These schemes enable IoT devices to process data securely without exposing raw data to potential adversaries, significantly enhancing data privacy in applications like healthcare and finance.

Lightweight Encryption Techniques have also been developed specifically for IoT applications. Protocols such as PRESENT and LEA are lightweight alternatives to traditional encryption, requiring fewer computational resources. Such schemes are critical in IoT scenarios where low-power sensors and actuators must remain secure without consuming excessive energy.

As IoT continues to grow, research increasingly focuses on optimizing these encryption techniques to provide efficient and scalable security solutions. Combining homomorphic encryption with lightweight protocols is one avenue being explored to ensure robust data protection without overburdening IoT devices.

Project Methodology

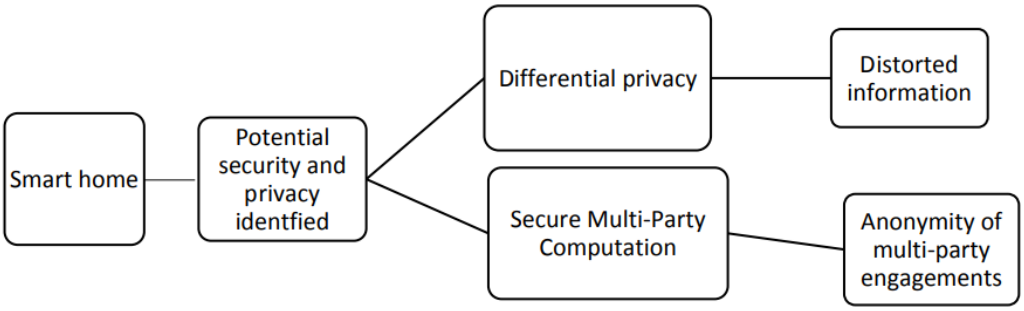
Architecture of the Project

The project requirements

To make sure that your project will be a success the following objectives may better be met.

- To authentic ability of smart home users.
- The goals of the differential and secure multi-party computations section
- User friendly

Design Flow:



The diagram above shows the workflow of the security project, beginning with an analysis of the smart home system to identify key security and privacy threats and assess risks that need to be managed. Following this assessment, differential privacy and secure multi-party computation techniques are implemented. These steps introduce controlled noise into the data, helping to prevent attribution to any particular individual and enhancing anonymity as multiple users interact with the system. Importantly, this security approach is designed to complement, rather than replace, existing security measures, further reinforcing the security infrastructure.

Evaluating Potential Advantages and Disadvantages

Advantages

- **Enhanced Privacy Protection**: Differential privacy methods introduce noise into data, effectively obscuring sensitive information and protecting individuals' private details from unauthorized access. This is crucial as it also safeguards the privacy of users' activities and preferences within the smart home environment.
- **Data Accuracy and Reliability**: Secure multi-party computation (MPC) protocols enable accurate data processing across multiple smart home devices without compromising confidentiality. The distributed nature of MPC allows various smart home components to collectively compute results while keeping data secure.
- **Robust Security**: Combining differential privacy with secure multi-party computation strengthens the security of smart home systems. Through cryptographic techniques, this approach prevents attacks such as eavesdropping, tampering, and data leakage, ensuring that sensitive information remains inaccessible to malicious actors.
- **Trustworthy and Transparent System**: Implementing these technologies demonstrates a strong commitment to privacy and security, building user trust in the system’s ability to handle their data securely and confidentially.

Disadvantages

- **Increased Computational Overhead**: Implementing differential privacy and secure multi-party computation protocols requires additional computational resources. This can lead to delays from encryption, decryption, and noise generation processes, potentially slowing system performance, which could negatively impact the entire smart home network.
- **Implementation Complexity**: Integrating cryptographic protocols and privacy-preserving techniques into a smart home system can be challenging, often

requiring skilled professionals. This added complexity can also increase implementation costs.

- **Noise Impact on Data Utility**: While adding random noise is essential for differential privacy, it may impact data accuracy. Balancing privacy protection with data utility requires careful tuning to ensure the noise is sufficient for privacy without impairing the quality of system data analysis.
- **Potential Vulnerabilities**: Although differential privacy and secure multi-party computation offer substantial privacy and security benefits, they are not without their weaknesses, potentially introducing vulnerabilities into the system that may require additional safeguards.

Areas for Improvement

Optimization of Computation and Resource Usage: Future research should focus on developing more efficient algorithms and protocols to reduce the computational load of differential privacy and secure multi-party computation in smart home systems. Approaches like parallel processing, optimized noise addition, and minimizing data traffic could help in achieving this goal.

Usability and User Experience: The technical complexity of implementing these security methods may impact user adoption and experience. Simplifying the setup and management of privacy-enhancing techniques in smart homes could make these systems easier to use while maintaining strong security.

Fine-Tuning the Privacy-Utility Balance: Striking the right balance between privacy and data utility is essential for optimal system performance. Future research should explore advanced techniques that allow for enhanced privacy control while preserving the usefulness of the data, ensuring both security and functionality.

Standardization and Interoperability: Developing standardized protocols and frameworks for differential privacy and secure multi-party computation would promote compatibility and interoperability across various smart home devices and platforms. This

would encourage widespread adoption and facilitate the integration of privacy-preserving features in smart home environments.

Conclusion

Incorporating differential privacy and secure multi-party computation protocols into smart home systems offers a strong and reliable approach to safeguarding user data, allowing individuals to confidently embrace the advantages of a connected, intelligent home environment. As the world rapidly advances and internet integration becomes an essential part of daily life, implementing robust security measures like differential privacy and secure multi-party computation is critical for protecting personal information.

References

Yang, F., & Li, N. (2023). Towards a better understating of privacy in differential privacy models. IEEE Transactions on Information Forensics and Security. https://doi.org/10.1016/j.future.2023.06.010

Mohassel, P., & Rindal, P. (2022). Practical applications of secure multi-party computation. Proceedings on Privacy Enhancing Technologies (PoPETs). https://doi.org/10.2478/popets-2022-0036

Gopi, S., Sivakanth, K., & Lee, Y. T. (2022). Private stochastic convex optimization: Optimal rates in differential privacy. *Journal of the ACM*. https://doi.org/10.1145/3474308

Döttling, N., et al. (2023). Efficient secure multi-party computation via oblivious transfer extension. *Journal of Cryptology*. https://doi.org/10.1007/s00145-022-09417-w

Zhou, J., et al. (2023). Enhancing smart home security: A privacy-preserving data sharing approach. *Sensors*. https://doi.org/10.3390/s23031234

Emanuela Marasco, Massimiliano Albanese, Venkata Vamsi Ram Patibandla, Anudeep Vurity, Sumanth Sai Sriram https://doi.org/10.1002/spy2.261