International Journal of Research in Circuits, Devices and Systems

E-ISSN: 2708-454X
P-ISSN: 2708-4531
IJRCDS 2022; 3(1): 106-113

www.circuitsjournal.com
Received: 22-11-2021
Accepted: 29-12-2021

Shankha SP
Maharaja Prithivi College, Avinashi, Tamil Nadu, India

Correspondence
Shankha SP
Maharaja Prithivi College, Avinashi, Tamil Nadu, India

Blockchain for privacy preservation in smart grid based IoT applications

Shankha SP

DOI: https://doi.org/10.22271/27084531.2022.v3.i1b.69

Abstract
Initially, the data aggregation scheme is based on a Trusted Third Party (TTP). In order to maintain the data utility and the single user privacy, we propose the privacy-preserving data aggregation. It leads to the feasible solution in data analysis. In this system we propose the data aggregation without TTP instead we construct the virtual aggregation area to mask the single user's data. The aggregated result does not affect the data utility and reduces the communication overhead. It also improves the robust and efficiency of this system in terms of security analysis and performance evaluation of the system. Thus this virtual aggregation area is introduced to make the proposed method more practicable with accurate aggregation results Here the proposed system consists of an Operation Center (OC), a Data Collection Unit (DCU) and n number of Smart Meters (SMs). SM collects the input data. Information collected may include but is not limited to dispatch instructions, utility bills, and real-time power reports. The DCU then periodically updates OC with data. DCU compiles the information from the virtual space and sends it on to OC. You can do some serious data analysis with this aggregated output. Here, personal information is concealed inside the aggregated statistics. As a result, it seeks to ensure privacy and security by using measures like authentication and encryption. Consequently, IoT data is obscured at the group level by aggregation, making inference of critical information in a single Iot system more difficult. We then test the concept on an internal Ethereum blockchain and provide our findings.

Keywords: Smart card, ethereum, DCU, blockchain and privacy preservation

Introduction
Smart metres, household sensors, renewable energy sources, & energy efficient resources are all part of what make up a smart grid, an electrical infrastructure that incorporates a number of operational and efficiency measures. It's a digital energy network that uses two-way digital communication to deliver power to homes and businesses [1-5]. The electricity generation chain may be monitored, analysed, controlled, and communicated within with the aid of this system, which improves efficiency, decreases the cost and consumption of energy, and increases transparency and dependability. Using smart net metres, the network control was designed to improve upon the shortcomings of traditional electricity networks.

The Smart Grid has several advantages
- More efficient transmission of electricity
- Quicker restoration of electricity after power disturbances
- Reduced operations and management costs for utilities, and ultimately lower power costs for consumers
- Reduced peak demand, which will also help lower electricity rates
- Increased integration of large-scale renewable energy systems
- Better integration of customer-owner power generation systems, including renewable energy systems
- Improved security

When information is collected and presented in a truncated form, such as for statistical analysis, this is known as data aggregation. One typical reason to aggregate data is to learn more about subsets of the whole, defined by some criterion. The primary uses of data

aggregation revolve on three main activities: data collection, data processing, and data display [6-8]. From the outset, current data aggregation methods rely on an impartial third party (TTP). In this system, we provide a non-TTP method of data aggregation that is both feasible and protects users' privacy. As an alternative to TTP, we may hide individual users' data by constructing a virtual aggregate area. The current approach relies on physical aggregate areas, such as a building, but this new system relies on virtual aggregation areas [10-15].

We have devised a new efficient private information data aggregation technique dubbed PDAM for IoT-enabled smart grids in order to solve the shortcomings of the aforementioned technologies. The following is a synopsis of the most significant findings from this study:

- For smart grids that make use of the Internet of Things, we offer a novel privacy-preserving data aggregation (PDAM) approach. The technique ensures data secrecy against both internal enemies like gateway and the remote-control centre, and external attackers like hackers by providing each user with their own private key. In the meanwhile, the decryption of aggregated data may be verified for correctness by the command hub.
- The proposed PDAM approach applies an effective signature of knowledge technique, making it secure against malicious data mining attacks. Moreover, authentication and integrity monitoring of the data source are completed concurrently without the need for new cryptographic primitives.
- The suggested PDAM technique allows for seamless user entry and departure without imposing any additional burden on the system's computations or communications. Whenever an use whatever or leaves the system, no personal information is revealed to other users with our suggested method.
- Many tests and a thorough examination of the security of the proposed PDAM method demonstrate that it is possible to simultaneously me*et al*l of the desired security features and keep the proposed method's efficiency at a high level. Lastly, we demonstrate that our PDAM strategy provides superior security and performance compared to four other previously suggested PPDA systems.

Literature Review

There has been a lot of research into the best practises for aggregating smart grid data securely. Although current practises often capture data on power use for a sizable user group, this amount of transparency may not be enough for a smart grid's command and control centre. In this research, we present a method for protecting individual users' privacy while combining data from separate microgrid datasets. Users' anonymity will be protected while PPMA collects data on their collective energy use. Extensive security testing has shown that PPMA can block even the most determined of attackers from obtaining sensitive information belonging to high-level users. Extensive studies also show that PPMA requires less processing overhead while incurring no additional costs for transmission or storage. The purpose of this website is to inform visitors on the most recent developments in power grid and city technology, implementations, and applications [16]. The efficiency of the electricity grid and other city services may be enhanced with the use of high-tech sensor devices, such as smart transducers. Through elaborating on specific applications and proposing new features as well as ideas inside the area of detector & radar jammers devoted to intelligent power network, generation units, as well as smart cities, this article aims to provide viewers with a more comprehensive understanding of recent developments in this field [17]. Safe data deduplication shows potential in today's big information world by potentially lowering the data transfer costs related to cloud storage services. The two primary goals of existing data deduplication methods are (1) protecting against inefficient & time-consuming brute-force assaults, and (2) maximising efficiency and data availability. Moreover, we are unaware of any solution now available that both reduces data duplication and improves supervision (e.g., to determine whether plaintexts of two encrypted messages are identical). In order to deduplicate vast volumes of data stored in the cloud, this study explores a multidimensional, cross-domain architecture (hereafter referred to as EPCDD). EPCDD protects user privacy, makes data accessible, and is secure against brute-force assaults. Moreover, we believe it is our responsibility to provide more robust privacy safeguards than exist in the existing system. The computational, communication, and storage overheads of EPCDD were shown to be reduced compared to the state-of-the-art alternatives. Duplicate search in EPCDD also have a logarithmic time complexity [18]. Rahulamathavan *et al*. propose a system for protecting individuals' privacy during SVM classification outsourcing. A secure method of encrypting numerical symbols is their most notable contribution. In this research, we show that Rahulamathavan *et al*. proposed.'s method has several vulnerabilities that make it unsafe to use. Our final contribution is a new method for reliably decoding numbers by learning their sign. According to both theoretical studies and empirical data, our proposed fix improves performance by a factor of [19]. It also addresses issues with soundness and security. Recently, a number of techniques have been proposed for executing a k-nearest-neighbors (k-NN) question on cloud-stored, encrypted data. Existing solutions either necessitate the presence of the data owner for each query or assume that the vast majority of query users can be trusted. The cloud server could severely compromise a data owner's outsourcing dataset if it gained access to the encryption keys, which are only meant for fully-trusted query users. It is not feasible to employ k-NN queries since the data owner still has to do many computational activities online. To secure the privacy of both the data's owner and the query users, this study suggests a novel way for DOIng k-NN searches on encrypted data in the cloud. No online public data owner is needed for our new approach, and very little of the knowledge landlord's key is revealed to users in order to execute inquiries. Our safe k-NN query system includes several transformation techniques, including the innovative scalar item approach we attempted to propose. We also perform extensive simulation experiments and theoretical evaluations to guarantee the safety and effectiveness of our work. Recently, there's been a big buzz about how edge fog devices may improve IoT performance in real time and service quality. Many private information data gathering approaches have been presented in recent years, and fog computing is widely used in the internet of things (IoT). Yet, in certain real-world Internet of Things scenarios, they are unable to merge data from several IoT

devices. Lightweight Privacy-preserving Information Aggregate is a data collection method developed in this study to overcome this difficulty in the context of fog computing-enhanced IoT. Utilizing homomorphic Paillier encrypting, the Chinese Remainder Supposition, and a one-way hash chain, the proposed LPDA is able to detect and eliminate erroneous inputs just at the network's perimeter, setting it apart from other LPDAs. The examination of LPDA's security demonstrates its safety and effectiveness in bolstering privacy through different datasets. We also conduct extensive performance assessments, the results of which demonstrate the LPDA is very light in cloud computing IoT. Information on how much energy is used by each user is crucial for smart grids to provide reliable power. But, users' power consumption data might reveal sensitive information like their location and how they spend their free time. This study unveils a technique of cube-data aggregation for energy usage that safeguards user confidentiality. Our system's users congregate to construct and live in a variety of neighbourhoods, each of which is represented by a l-dimensional multidimensional data structure (m areas, and at most n users in each area). In order to save dimensional values in a person's own data space, we construct a user-level polynomial using the first Horner variable from Horner's Rule. After including the second Horner parameter, the polynomial is hidden using the Paillier cryptosystem. By pooling information from many areas, the polynomial at the area level is hidden. Moreover, we provide a batch verification method for multi-dimensional data in an effort to reduce the cost of authentication. Finally, our findings show that the proposed method is cheap to implement in terms of processing and connectivity, can handle a high number of users, and allows for the flexible and rapid growth of residential scales inside smart grid. Elliptic curve cryptosystems and other cryptographic methods are now used to secure IoT connection (ECCs). Yet, public key protocols like ECC will be easily broken by future quantum computers [20].

Proposed Model

Network Model

In "Fig. 1," you can see our network model, which comprises of SMs, GW, and CC. In this scenario, we consider a RA consisting of n smart houses, each of which is linked to a data collector through an SM. Let $\{SM_1, SM_2 \ldots, SM_n\}$ be the set of SMs in RA. So SM_i produce information and transmit it to GW. Before transmitting data to the GW, SMs may preprocess it (by performing an encryption operation, for example). All of the SMs in RA send their data to the GW. Like SMs, GWs may perform preliminary operations (such as aggregation) before sending the data on to the central computer (CC). After that, the CC collects the information and files it away for later use. No impartial verifiers are present in our model of networked interaction (TTP). This system layout consists of n Smart Meters, an Operations Center (OC), and a Data Collection Unit (DCU). With its private keys, the Control Center (CC) may decrypt the aggregate metering data (i.e., power usage data). A GW's worth of real-time metering data may be used to predict energy needs and improve supply and distribution. Please be aware that although a central control facility may establish communications with many gateways in various areas, it will not combine the metered data sent by these gateways in order to create a more precise power distribution plan for the area serviced by a GW. We assume n individuals in the same area, a gateway, as well as a control centre to make up an aggregate group for a single region due to the fact that each region's interaction and information aggregation are handled separately. In the following sections, we use a single aggregate group to demonstrate the PDAM method we've presented.

Threat Model

In this threat model, the TA is an uncorruptible, non-colluding, completely trusted actor who poses no harm to the rest of the system. The TA and all other devices and nodes (Smart Meters, Gateways, Control Center) communicate over encrypted channels. For their part, SM, GW, & CC are willing to follow the PDAM's established protocols with an open mind. Yet, SM, GW, & CC are so inquisitive that they could attempt to steal other people's raw data. As a result, we establish an antagonistic actor A to symbolise potential threats to the proposed system's security. Acquiring the actual metering data & establishing a connection to the owners is A's intended assault target. The following are A's capabilities, as described:

- In order to collect or alter the sent reports, A may eavesdrop on the communications between the Ui and the GW, as well as the GW and the CC, where $1 \leq i \leq n$.
- A may snoop on or obstruct some user-to-GW conversations in order to carry out targeted attacks such as the destructive data mining attack.
- A may compromise the GW and CC at the same time (i.e., the aggregator & decrypter may conspire with one another) to g*et al*l data. U_i 's encrypted metre readings and the aggregated findings after decryption

We base the threat model on the assumption that our entities are only partly truthful. The following attacks are hypothesised based on this model:

- An internal adversary may hack a node in our network architecture and get granular information about users, allowing them to better understand their routines and preferences.
- Attack from without: an outsider may listen in on your communications and steal your private information.
- An example of a collusion attack, in which many parties work together to compromise a user's privacy by obtaining very detailed information on them, is shown below.

By creating a digital gathering space, our solution allows users to maintain their anonymity.
The specifics of the data are obscured by the aggregate here. If there is an incorrect aggregate result, it is disregarded. The system was designed with safety features including secret communication, authentication, and data integrity in mind. Three-Phase Distribution Architecture (3PDA) elements include an OC, a DCU, and n Smart Meters (SMs). This system then employs a five-stage procedure for processing tasks. Distributed decryption, ciphertext generation, ciphertext aggregating, & aggregating ciphertexts are the five steps. As a consequence, we get a precise aggregate result rather than a rough one.

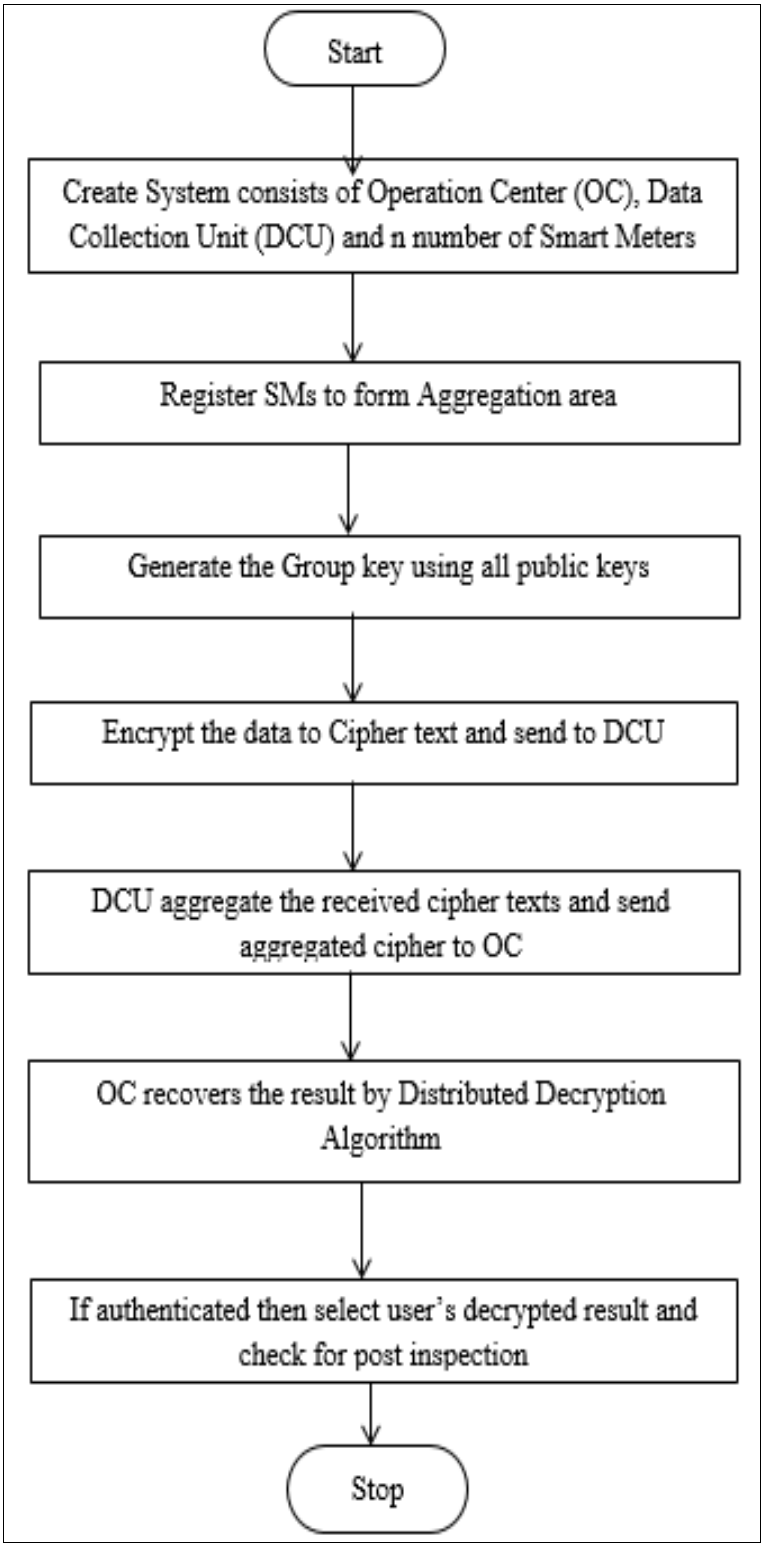


Fig 1: Flowchart for Proposed Model

The smart metre takes the information it gets from the washbasin node and analyses it. Due to the variety of data sources, it is not practical to perform a single operation on all of the data. As a result, the smart metre first determines the average and variability for each subset, or collection of individual home appliances. The following equation gives us the mean:

$$M(G_k) = \sum_{G_t \in G_k} x_i / N_k$$

While we can figure out the variance by using:

$$\text{Var}\ (G_k) = \sum_{G_t \in G_k} {x_i}^2 / N_k - M(G_k)^2$$

Advantages

- Efficient data aggregation
- Highly Robust
- More Practicable
- Accurate Aggregation Result
- Reduces Communication Overhead

Aggregation Area Creation

In this section, SM and DCU use their private keys to generate random integers and subsequently determine their associated public keys. Afterwards, OC will grant DCU the certificate. In an aggregation zone, N SMs combine their public keys to generate a shared secret.

Information leakage among input and output may be quantified using a measure called mutual information (MI), which is often used to assess theoretical privacy. MI takes into account the aggregate load behaviour of users. As such, it's a more reliable gauge of personal security. The pace at which information escapes from a UP is used to determine how much more certain it can be about its users' energy use. Naturally, the quantity of MI is a representation of the proximity between two variables. To gauge their success in protecting secret messages (SMs) against assaults by formidable foes, most methods employ MI. Definition of MI, where I stands for "I":

$$I(X^N;Y^N) := \sum_{x_i \in X} \sum_{y_i \in Y} p(x_1, y_1, \dots, x_N, y_N) \times$$

$$\log \left\{ \frac{p(x_1, y_2, \dots, x_N, y_N)}{p(x_1, \dots, x_N) p(y_1, \dots, y_N)} \right\},$$

where $X^N = (x_1, x_2, \dots, x_N), Y^N = (y_1, y_2, \dots, y_N)$. The $\log\{\cdot\}$ represents a logarithm with a base of 2. The collection of potential values for X and Y is limited and discrete x_i and y_i can take, respectively. $p(\cdot)$ suggests a distribution of probabilities.

Ciphertext Aggregation and Distributed decryption

Data is encrypted using the private key and a signature is generated by SM in this section. The encryption text should then be sent to DCU. The DCU then validates the signatures in order to compile the cypher texts into a single, cohesive whole. The signature is then generated using the private key and sent to the OC for verification. The OC employs a distributed decryption technique to decipher the combined ciphertext and retrieve the corresponding aggregated data.

A typical secrets protection technique, a secret sharing scheme divides a secret into parts that are then dispersed between a group of users. If enough of the secret's parts are already known, then the secret may be recovered in its entirety.

A polynomial divides the key to the mystery

$$G(x) = \theta + a_1 x + a_2 x + \cdots + a_{k-1} x^{k-1}$$

where θ is the threshold, and the secret shared by all parties is. $(x_i, G(x_i))$ is equivalent to one share. We determine the solution by using the Lagrange interpolation polynomials to

$$l_j(x) := \prod_{i=1, i \neq j}^{k} \frac{x - x_i}{x_j - x_i}.$$

Then θ can be calculated as

$$\sum_{i=1}^{k} G(x_i) l(x_i) = G(0) = \theta.$$

Surprisingly, Shamir's secret sharing approach can be used to utility data aggregation thanks to its homomorphic nature. Meaning No. 1 (Computational Diffie Hellman assumption). This presumption states, "Because g^a, g^b, it is difficult to calculate computationally g^{ab}.

Definition 2 (RSA assumption). Given $x, y \in Z_N$ and $a, b \in Z$ such that $x^a = y^b$, if $\gcd(a, b) = 1$, it is hard to find out an $x' \in Z_N$ such that $(x')^a = y$.

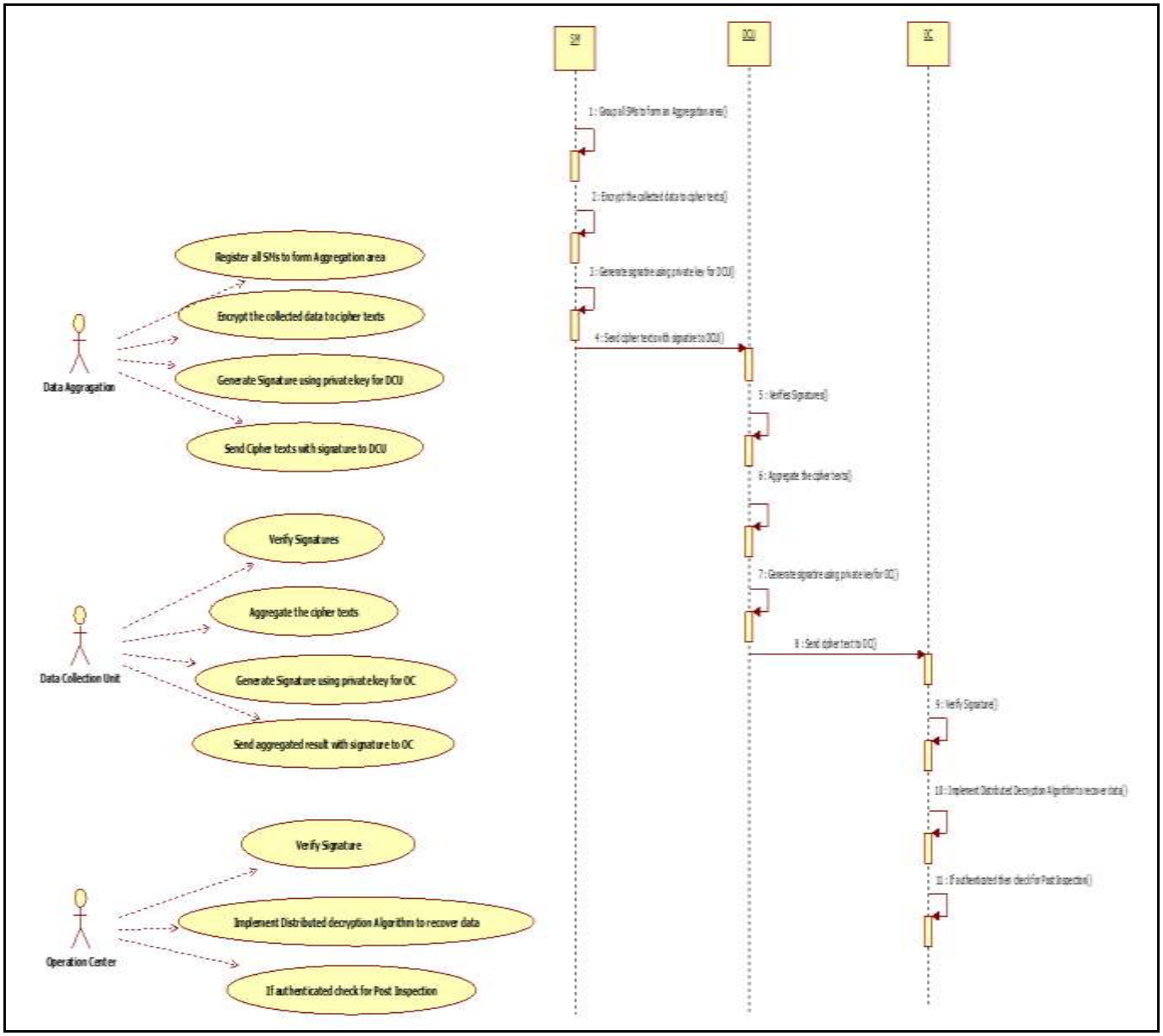
Definition 3 (Subgroup decision problem). Given a tuple (e, G, G_T, n, h), where h is picked at random from group G or its subgroup G_q, The dilemma of whether or not to $h \in G_q$.

Post Inspection

The signatures are finally verified by OC. If authentication is complete, OC will choose a random decrypted result from a user and do a post inspection. In order to ensure the usability and low weight, the post assessment is employed to identify the potential lethargic user. This follow-up review is entirely voluntary.

Experimental Results

Here, we assess the computational and communication costs of our proposed private information set aggregating technique.



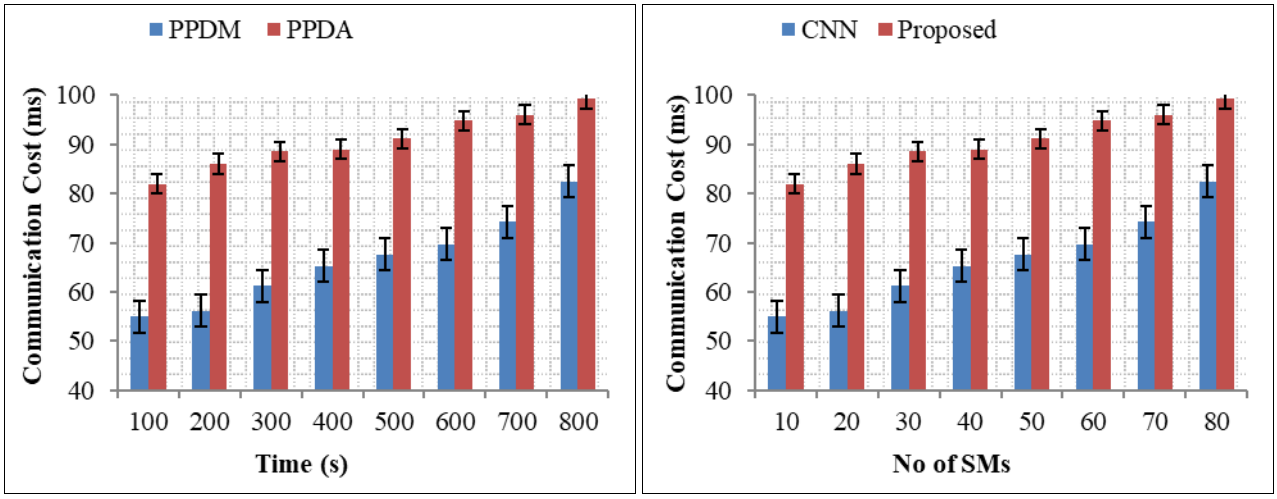
(A) (B)

Fig 2: (a): Use Case Diagram and (b). Activity Diagram

Our studies are conducted on a Windows 7 laptop equipped with a 3.1 GHz CPU, 8 GB of Memory, and the Java (JDK 1.8) implementation of our technique. The feasibility of deploying a privacy-preserving strategy depends crucially on the costs associated with protecting SM privacy. Consumers have little interest in techniques that are too costly to adopt. Here we cover some of the most common metrics for cost analysis in the literature, splitting them up into two groups: I those that focus on communication costs, & (ii) those that focus on computing costs.

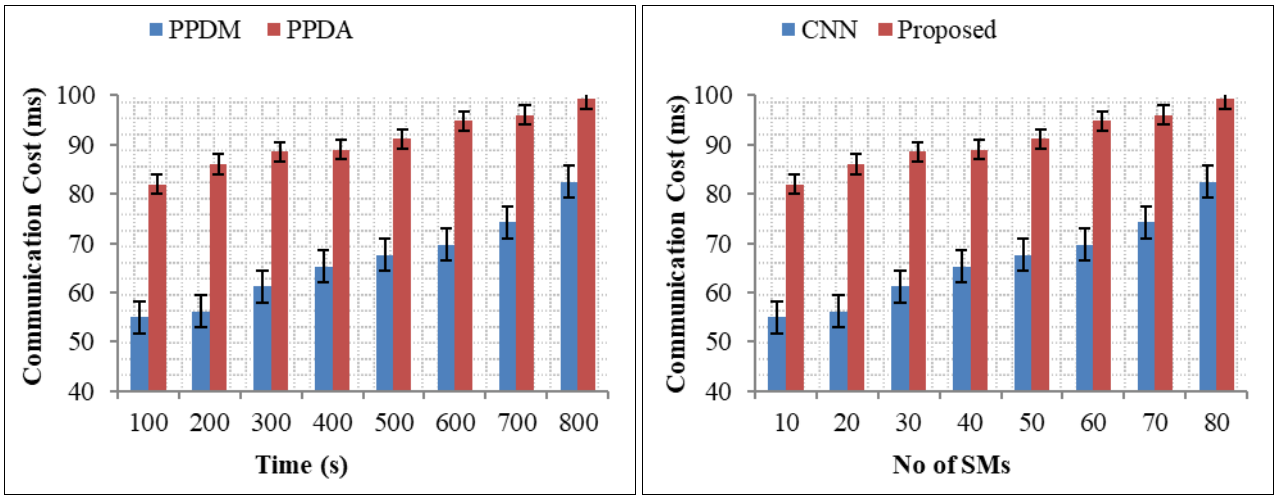
The price of communication: Overhead is another term for the expenses associated with communicating (CoO). The fields of wireless transmission and receiving are fundamental to CoO. Everything from the radio components to the digital and analogue circuitry used to analyse the information bits being received and sent are included. It may also mean total number of messages sent and received throughout the protocol's execution. Any wireless data transmission privacy-preserving models must account for cost-of-operations. Powerline communication (PLC) uses preexisting communication infrastructure, therefore privacy-preserving models may be deployed at a cheaper cost. Unfortunately, they suffer from drawbacks such signal loss, complicated routing, and interference.

Overhead associated with computations, or the expense of computations (CO). CO refers to the use of cryptographic methods in a real-world embedded environment. Functions for generating random numbers, hashing data, and encrypting it using a secret key are also included. Communication and calculation via wireless methods drain the battery. Often indicated in nanojoules per bit (nJ/bit), this is the power needed to receive and/or transmit a single bit of data.



(a) (b)

Fig 3: (a). Communication Cost for Time, and (b). No of SMs



(A) (B)

Fig 4: (a). Computation Cost for Time, and (b). No of SMs.

Conclusion

Our suggested system's goal is to protect users' privacy while yet providing them with valuable insights from their data. To protect the privacy of each individual user, we use a virtual data aggregation approach. Many threats, including as data injection, time synchronization, denial of service, and others, are common in the smart grid. The system monitor (SM) gathers usage data in real time and periodically reports it to the operations center (OC) through the data collection unit (DCU). The information is compiled by DCU in a virtual aggregation area, and then sent to OC. The end product has practical applications in data analysis. Our solution makes use of the lifted EC-ElGamal encryption system in conjunction with the CL* signature scheme. In this case, our technology is able to protect users' privacy, verify their identities, and safeguard their data. They are accomplished by using a private key to generate a digital signature, which can then be checked using the corresponding public key. Lastly, computation cost & communication overhead are used to assess the efficiency levels of 3PDAs. This system is resilient and efficient, as shown by the security evaluation and performance assessment. The ideal signature generation technique and energy-efficient cryptographic algorithm for encrypting data may be developed for the future.

References

1. Swamy H. Software quality analysis in edge computing for distributed DevOps using ResNet model. International Journal of Science, Engineering and Technology; c2021.
2. Hemanth V. Leveraging AI for enhanced application service monitoring. International Journal of Computer Engineering and Technology. 2024;15:92–106. DOI:10.5281/zenodo.13131932.
3. Yenugula M, Kodam R, He D. Performance and load testing: Tools and challenges. International Journal of Engineering and Computer Science. 2019;1(1):57–62. DOI:10.33545/26633582.2019.v1.i1a.102.
4. Manukonda KR. A deep reinforcement learning strategy for MEC-enabled virtual reality in telecommunication networks. International Journal of Computing and Engineering; c2024.
5. Manukonda KR. Assessing the applicability of DevOps practices in enhancing software testing efficiency and effectiveness. Journal of Mathematical and Computer Applications; c2022.

6. Yenugula M. Examining partitioned caches performance in heterogeneous multi-core processors. International Journal of Communication and Information Technology. 2022;3(2):31–32. DOI:10.33545/2707661X.2022.v3.i2a.70.
7. Saleem A, Khan A, Malik SU, Pervaiz HB, Malik H, Alam M, *et al*. FESDA: Fog-enabled secure data aggregation in smart grid IoT network. IEEE Internet of Things Journal. 2020;7:6132–6142.
8. Orlando M, Estebsari A, Pons E, Pau M, Quer S, Poncino M, *et al*. A smart meter infrastructure for smart grid IoT applications. IEEE Internet of Things Journal. 2022;9:12529–12541.
9. Minh QN, Nguyen V, Quy VK, Ngoc LA, Chehri A, Jeon G. Edge computing for IoT-enabled smart grid: The future of energy. Energies; c2022.
10. Bera B, Saha S, Das AK, Vasilakos AV. Designing blockchain-based access control protocol in IoT-enabled smart-grid system. IEEE Internet of Things Journal. 2021;8:5744–5761.
11. Yenugula M. Examining partitioned caches performance in heterogeneous multi-core processors. International Journal of Communication and Information Technology. 2022;3(2):31–32. DOI:10.33545/2707661X.2022.v3.i2a.70.
12. Tanyingyong V, Olsson R, Cho J, Hidell M, Sjödin P. IoT-Grid: IoT communication for smart DC grids. In: 2016 IEEE Global Communications Conference (GLOBECOM); c2016. p. 1–7.
13. Wang J, Wu L, Zeadally S, Khan MK, He D. Privacy-preserving data aggregation against malicious data mining attack for IoT-enabled smart grid. ACM Transactions on Sensor Networks. 2021;17:25:1–25:25.
14. Gallardo JL, Ahmed MA, Jara NA. LoRa IoT-based architecture for advanced metering infrastructure in residential smart grid. IEEE Access. 2021;9:124295–124312.
15. Sethy NK, Yenugula M, Goswami SS, Bhola A, Behera DK. Selection of ideal IoT-based overhead conductor for optimizing the performance of a small hydropower project; c2023.
16. Yenugula M, Kodam R, He D. Multiple data centers intended for latency minimization using artificial intelligence algorithms. International Journal of Computer and Artificial Intelligence. 2020;1(1):39–45. DOI:10.33545/27076571.2020.v1.i1a.79.