HBFZKP: A DUAL PRIVACY PROTECTION MODEL LOCATION BASED SERVICE SYSTEMS

KHALID ALSUBHI

Department of Computer Science, King Abdulaziz University, Saudi Arabia

E-mail: kalsubhi@kau.edu.sa

ABSTRACT

Location-based services (LBS) have become pervasive, reaching all smart devices equipped with GPS, delivering substantial value to consumers. Despite their popularity, LBS has its shortcomings, particularly concerning the necessity for users to disclose their location data to fully benefit from the service, potentially compromising their privacy and security. As a result, numerous techniques have been proposed in the literature to offer an optimal solution for preserving privacy in LBS queries. This study will initially delve into three established approaches commonly employed for safeguarding privacy in location-based services: Zero Knowledge Proof, Oblivious Transfer, and the Bloom filter. Each of these methods aims to minimize the disclosure of information while simultaneously establishing an automated performance metric. Among the three methods mentioned, Bloom filters arguably exhibit the most efficient runtime performance. Nonetheless, Bloom filters exhibit two drawbacks: (a) they leak a maximum of one bit of information per query, and (b) the hash functions (Hk) require meticulous design and security analysis to ensure they are orthogonal and independent. This signifies that if one H is compromised (secure), nothing can be deduced about any other H, preserving the integrity of the remaining hash functions. In response to these challenges, we propose an innovative two-phase privacy-preserving framework for LBS, hybrid of Bloom filter and Zero Knowledge Proof (HBfZkp). While all three of these methods have demonstrated their efficacy in safeguarding a user's private data, our proposed two-phase privacy approach is poised to elevate privacy protection further. It is designed to shield users from both internal and external threats by capitalizing on the inherent strengths of Zero Knowledge Proof and Oblivious Transfer in safeguarding against these distinct types of attacks, respectively.

Keywords: *LBS, Privacy, Bloom Filter, Zero Knowledge.*

1. INTRODUCTION

The objective of making queries to a location-based service while safeguarding privacy and efficiency presents a set of intricate security challenges. The first challenge pertains to implementation: Can we structure queries to a data store, be it a service, database, or website, in a way that divulges the least information to the data store while maximizing the user's utility? For a long time, it was perceived as a daunting task, if not impossible, to reconcile these conflicting requirements. Nevertheless, recent research has revealed the feasibility of various query protocols that can, at least probabilistically, strike a balance between these objectives.

Another concern arises when we contemplate the potential compromise of the server or its overtly malicious intent. Can we design queries in a manner that guarantees responses that cannot be forged, making it impossible for the server to generate counterfeit responses that appear genuine? Even in the presence of a malicious server, eavesdropper, or man-in-the-middle attacker, the existence of "1-in-q" algorithms has paved the way for security protocols that can offer probabilistic assurances regarding the authenticity of responses. A significant cryptographic breakthrough recently introduced fully homomorphic encryption (FHE), wherein the data store processes encrypted data without access to unencrypted information, ensuring that responses are genuinely unforgeable, not just probabilistically so. This brings us to the third concern in privacy-preserving queries, which is efficiency. "1-in-q" algorithms can provide runtime performance on the order of O(n) or even O(1), allowing the strength of the probabilistic guarantee to align with the user's privacy goals. The accuracy of the response can be improved by incurring a linear or constant-time computational overhead. While partially homomorphic encryption schemes, such as Routing and Spectrum Allocation (RSA), can exhibit exponential computational growth, years of experience have yielded implementation heuristics that largely prevent exponential complexity, ensuring computations remain polynomial except with negligible probability. In contrast, efficient computation for FHE is currently immature, with even simple FHE computations potentially taking several seconds. This level of performance is presently unsuitable for end-user utilization.

Finally, it's crucial to consider the unique requirements associated with location-based data. LBS query responses consist of multiple data items, making it easier for malicious actors like man-in-the-middle eavesdroppers to correlate multiple queries, potentially compromising privacy. Any privacy-preserving solution for location-based servers must address this behavior.

The subsequent sections of this document will outline three possible approaches to address these challenges: zero knowledge proofs (ZKPs), oblivious transfer protocols (OT), and Bloom filters (BF). A compelling argument can be made that these diverse protocols can be effectively combined to create solutions stronger than any individual approach.

Our contribution

- Propose a 1-bit security guarantee achievable through a combination of a Zero-Knowledge Proof System (for internal attacks) and Oblivious Transfer (for external attacks).
- Devise Privacy-Preserving Queries tailored for Location-Based Services using the principles of Bloom Filters.
- Create an algorithm, denoted as "A," whether it relies on Zero-Knowledge Proofs (ZKP) or Oblivious Transfer (OT), aimed at minimizing information leakage to 1 bit per query within a pure Bloom Filter (BF) system. Additionally, formulate an automated performance metric that can be computed through simulated execution of the composite algorithm to probabilistically quantify the value of N. Demonstrate that for a well-optimized A, N can significantly exceed 1.
- Develop an advanced procedure that transforms algorithm A, initially designed for value types, into a functional A that operates on function types. Establish two performance measures that calculate the overall entropy and mutual information of a sequence of hash functions before A's transformation and after it. Create a simulation that computes these measures.
- Conduct a comprehensive evaluation of the proposed approach concerning security and privacy efficiency.

2. RELATED WORK

In reference to [33], Information Access Control serves as a technique aimed at preserving the location privacy of LBS (Location-Based Services) users. This approach hinges on granting LBS users the ability to regulate access to their location data. To achieve this, LBS providers enforce the utilization of access policies to govern access to users' location data. However, a drawback of this technique is the potential misuse of location data by LBS providers who could act as adversaries.

Another technique known as the Mix Zone, described in [34], relies on an intermediate server to obfuscate a user's location. When a user enters a mix zone, they are assigned a pseudonym, which is then used to submit queries to the LBS server via the intermediary server. The user receives a new pseudonym when they leave the mix zone. Although this method is applicable in scenarios like road networks, its vulnerability lies in the risk of compromise of the intermediate server by adversaries. In [35, 36], the k-anonymity technique is employed to protect location privacy. This method involves grouping mobile users into clusters of k members, defining a bounding region for each group, and having users use the bounding region as their location when making queries to the LBS provider. The intermediate server assists in constructing the bounding region. While this technique makes it challenging for adversaries to pinpoint a user's exact location, it is not immune to potential compromise of the intermediate server.

Another approach, discussed in [37, 38], involves the use of dummy locations. In this method, a mobile user confuses the LBS server by sending multiple queries, with one containing their real location and the rest containing fake locations. However, adversaries may leverage side information to identify the dummy locations, making this technique susceptible to exploitation. [39] and [40] introduce the concept of geographic data transformation. Users own a location dataset, and to share it, a transformation process is applied using a secret key. This transformed dataset, hosted by an LBS server, is ready for sharing. While this transformation process enhances location privacy, there is a risk of adversaries analyzing access patterns for the transformed locations to potentially compromise the real location data. Private Information Retrieval (PIR) is another technique discussed in [41], [42], [43]. It uses cryptographic systems to enable users to access LBS server database records without revealing which specific record is being accessed. However, this approach relies on dedicated hardware with embedded secret keys, posing a potential risk if hardware manufacturers compromise location privacy.

In [44], an optimal approach to address current location-based query challenges, particularly data leakage in query databases, is proposed. The authors suggest a two-stage approach involving Oblivious Transfer and Private Information Retrieval. They evaluate the method's efficiency using a desktop machine and a mobile device. Authors in [45] introduce the Privacy-Preserving Location Proof Updating System (APPLAUS), focusing on co-located Bluetooth-enabled mobile devices to generate location proofs and update a location proof server. They use periodically changed pseudonyms to enhance security and offer users control over their location privacy levels.

In [46], the focus is on managing privacy protection and LBS accuracy based on population and road density. The authors propose a context-aware LBS system with integrated data privacy and communication anonymity, demonstrating its efficiency on Google Maps. Authors in [14] address the query linking problem in preserving mobile users' privacy within LBS. They introduce the V-DCA algorithm, which combines user rapidity, acceleration, and cloaked groups to enhance privacy while reducing algorithm complexity. [47] introduces a Private Set Intersection (PSI) protocol based on oblivious Bloom intersection, offering scalability and security in semi-honest and malicious models. [48] focuses on location sharing services in online social networks (mOSNs) and presents BMobishare, a security-enhanced privacy-preserving location sharing mechanism using Bloom Filters. In [49], a privacy mechanism is designed for LBS in vehicular ad hoc networks (VANET). The authors propose a privacy mechanism based on multi-party computation and zero-knowledge proofs to protect location information. [50] presents a zero-knowledge multi-copy routing algorithm for mobile social networks (MSNs), with a focus on community homes spread messages. Authors in [51] address password-guessing attacks and propose an enhanced Kerberos protocol based on public key cryptography. [52] employs middleware to generate client certificates for pseudonymous usage, while [53] introduces an anonymous authentication system. [54] suggests the use of zero-knowledge proofs and RSA cryptography in web browser login systems to prevent password attacks. [55] explores the application of tamper-proof hardware for universally composable secure computation, presenting efficient oblivious transfer protocols. [56] discusses protocols for privacy-preserving computation using oblivious transfer, k-anonymous oblivious transfer, deterministic encryption, and Bloom Filters. [57] introduces interactive hashing as a cryptographic primitive and demonstrates the benefits of interactive hashing in secure computation. [58] discusses oblivious transfer extensions and presents an efficient OT extension protocol for secure computation. [59] focuses on privacy in mobile social networks, offering a customized privacy mechanism for user profiles and communication. [60] introduces the spatial Bloom filter (SBF) to store location information and presents privacy-preserving protocols for location-aware applications. [61] addresses the need for location privacy in location-aware applications and introduces the spatial Bloom filter (SBF) to manage location data. [62] presents an approach that combines Bloom filters and hash tables to enhance the efficiency of Bloom filters in representing sets.

3. PROPOSED PRIVACY FRAMEWORK

Among the three methods mentioned earlier, Bloom Filters indeed stand out in terms of runtime performance. However, they do have two significant shortcomings:

To address these deficiencies, our proposed approach involves combining a Bloom Filter with a second technique, which could be either Zero-Knowledge Proofs (ZKP) or Oblivious Transfer (OT). In the proposed approach, we explore two methods for combining privacy techniques: ZKP+BF and OT+BF. The objectives for both of these approaches are consistent:

- ***Reducing Information Leakage:*** The primary aim is to asymptotically decrease the amount of information that the Bloom Filter (BF) leaks, from 1 bit per query to 1 bit per N queries, for N that can be arbitrarily large. This reduction is crucial for enhancing privacy and security.
- ***Generating Independent Hash Functions:*** Another key goal is to create a mechanism, often referred to as an "engine," that can produce a set of hash functions that are both orthogonal and independent.

a) Information Leakage: Bloom Filters can leak at most one bit of information per query. This means that, in certain cases, an observer could potentially gain some insight or infer partial information from the queries made.

b) Hash Function Security: The hash functions (Hk) used in Bloom Filters need to be designed with careful attention to security. They should be orthogonal and independent from each other. In essence, even if one of these hash functions (let's say Hi) is compromised or broken, it should not reveal any information about the other hash functions (Hj) where j is not equal to i. This is crucial to ensure that the compromise of one hash function does not lead to the breach of the entire system. These hash functions should satisfy a specific property, where the joint distribution P(Hi|Hj) - P(Hi) - P(Hj) is bounded from above by an extremely small value denoted as E. It should be such that there is an exceedingly low probability of finding any x, y for which:

$$\| P(Hi(x)|Hj(y)) - P(Hi(x)) - P(Hj(y)) \| > E \qquad (1)$$

In this equation, P(Hi(x)) signifies the likelihood of successfully reversing or inverting the hash function Hi, meaning the probability of discovering any x' such that Hi(x') = Hi(x). Developing such hash function generators, often referred to as "mixmasters," is recognized to be a challenging problem in the field of cryptography and privacy. Figure 1 presents a block diagram of proposed hybrid technique to secure LBS privacy.

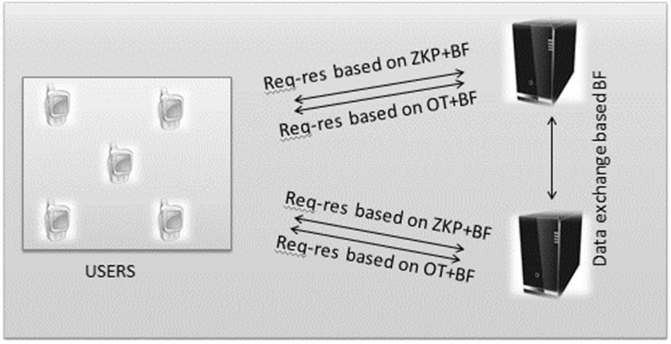

Figure 1. *Block Diagram Of Proposed Hybrid Method For LBS Privacy Provisioning*

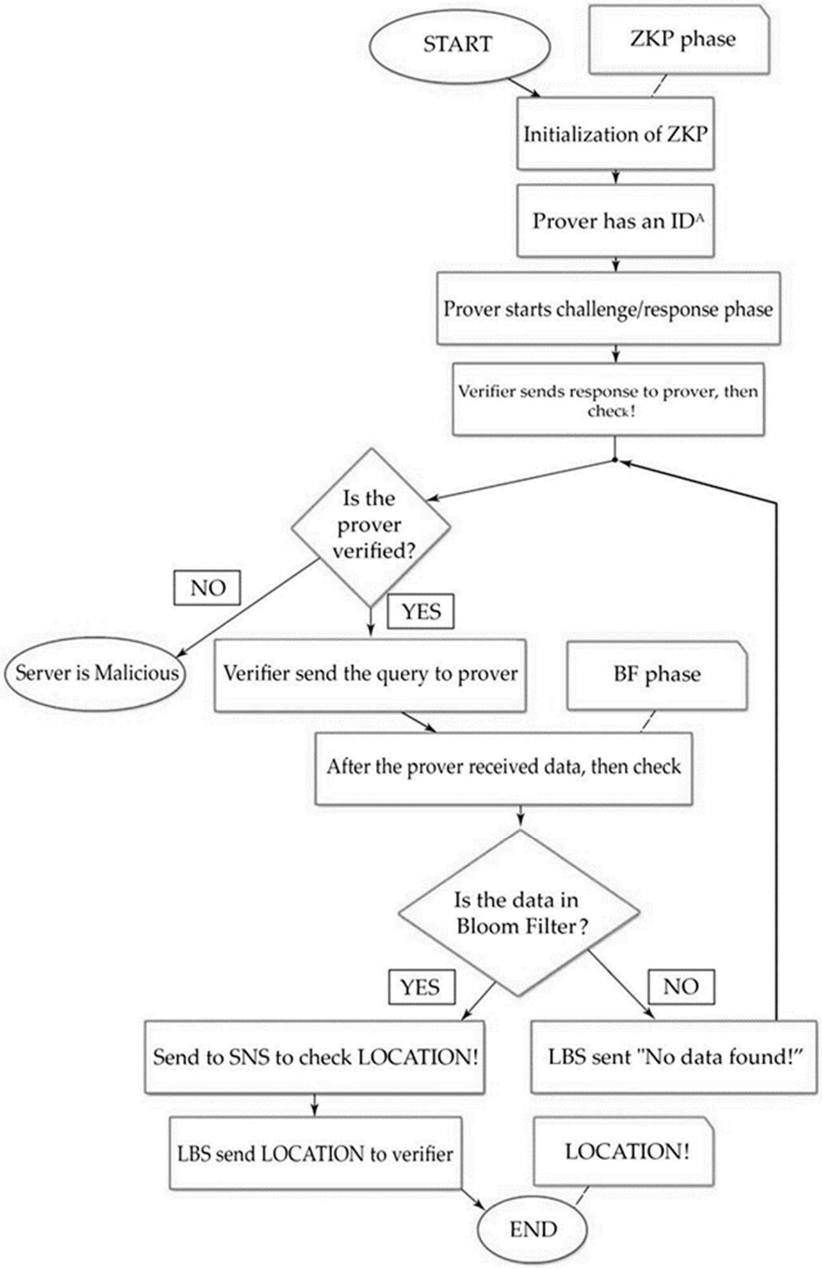
START
ZKP phase
Initialization of ZKP
Prover has an ID^A
Prover starts challenge/response phase
Verifier sends response to prover, then check!
Is the prover verified?
NO
YES
Server is Malicious
Verifier send the query to prover
BF phase
After the prover received data, then check
Is the data in Bloom Filter?
YES
NO
Send to SNS to check LOCATION!
LBS sent "No data found!"
LBS send LOCATION to verifier
LOCATION!
END

Figure 2. Flow Diagram Of Proposed Hbfzkp Method For LBS Privacy Provisioning

Algorithm 1. Secure Location Data Storage Using Hybrid ZKP And BF:

Step 1: Secure Location Data Storage using Bloom Filters:

- User location data is hashed and securely stored within a Bloom Filter.
- Bloom Filters provide an efficient way to query and retrieve location data, reducing response times.

Step 2: Privacy-Preserving Query Authentication with ZKPs:

- When a user queries the LBS, they generate a ZKP attesting to their proximity to a specific location without disclosing the exact coordinates.
- The ZKP allows the LBS to authenticate the user's query without learning sensitive location information.

Step 3: Integration of Bloom Filters and ZKPs:

- The user query is processed through the Bloom Filter to identify potential matching locations, minimizing false positives.
- The ZKP is then used to verify the user's proximity to these potential matches, providing an additional layer of privacy protection.

4. SECURITY ANALYSIS

Let: "BF" represents the Bloom Filter, "Q" be a user's query, "P(x)" represent the presence of an element x in the Bloom Filter, "ZKP(Q)" denote the Zero Knowledge Proof for query Q:

$$\text{Verify}(Q) = (\text{ZKP}(Q) \text{ AND } P(Q)) \text{ OR } \neg\text{ZKP}(Q) \quad (2)$$

In above equation, Verify(Q) indicates the result of the algorithm for query Q. ZKP(Q) represents the Zero Knowledge Proof for query Q. P(Q) denotes the presence of the user's query Q in the Bloom Filter. AND and OR are logical operators.

The proposed data transfer protocol enables secure and privacy-preserving interactions between an LBS client and an LBS server. It is designed to meet the five specified properties while allowing the client to make location-based queries and obtain proofs of assertions with varying levels of confidence.

Protocol Properties:

Proof of Assertion (p):

The protocol should incorporate a Zero Knowledge Proof (ZKP) system. Each query issued by the client must include a ZKP component that demonstrates the validity of the assertion without revealing sensitive information. The probability (p) of successfully proving the assertion should be set as a parameter. This component will be cryptographically verifiable by the server.

Exponential Increase in Confidence (p):

To increase the confidence (p) exponentially, the protocol will support a feature where the client can issue multiple queries in a sequential manner. The server will provide independent ZKP responses for each query. The client can then combine these proofs to increase the confidence exponentially in a straightforward way.

Information Leakage (Negligible Probability):

To minimize information leakage, Bloom Filters will be used. The queries will be processed using Bloom Filters to obfuscate the query and response patterns. The leakage probability will be made negligible through the appropriate design of the Bloom Filters and query handling mechanisms.

Malicious LBS Server Detection (q):

The protocol will incorporate a reputation system for LBS servers. Each query response from the server will include a unique digital signature. The client will keep a record of responses and verify them over time. If any response is found to be inconsistent or suspicious, it will contribute to the calculation of the malicious server detection probability (q).

Exponential Increase in Detection Confidence (q):

The client can enhance its ability to detect a malicious server by continually interacting with the same server. The cumulative probability of detecting a malicious server (q) can be exponentially increased by collecting a sufficient number of query responses and evaluating the server's consistency and integrity over time.

Protocol Workflow:

Query Generation: The LBS client generates a location-based query and computes an associated ZKP proof for the assertion.

Query Transmission: The client transmits the query and the ZKP proof to the LBS server.

Server Verification: The LBS server verifies the ZKP proof and processes the query while maintaining user privacy using Bloom Filters.

Response Generation: The server generates a response, signs it with a unique digital signature, and sends it back to the client.

Response Verification: The client receives the response and verifies the server's digital signature. The response is stored for future reference.

Iterative Querying: The client may choose to repeat the process by issuing multiple queries to the server to increase confidence in the assertion's validity and detect malicious behavior.

- The protocol provides strong security and privacy guarantees:
- Zero Knowledge Proofs ensure the privacy of user assertions.
- Bloom Filters minimize information leakage.
- The reputation system helps detect malicious servers.
- The ability to issue multiple queries exponentially increases the confidence in the assertion's validity.

5. IMPLEMENTATION AND RESULTS

In this section, we assess our proposed privacy provisioning hybrid ZKP and BF scheme. Taking into account the perspectives of the Location-Based Service Provider (LBSP), the LBS user, and the Cloud Service Provider (CSP). The software and hardware configurations for the LBSP and LBS user sides were executed on a 64-bit Ubuntu12.04 LTS system equipped with an Intel Core i7 processor and 16GB of RAM. On the CSP side, a virtual machine was employed, running an Intel Xeon processor E5-4600, with 16 GB of memory on a Dell blade server M830. VMware vSphere ESXi was utilized to establish a private cloud environment. The implementation of pairing group operations was achieved using the open-source Charm library [34], which leverages standard PBC library support [35] and FLINT [36] for finite field arithmetic within Zn*.

To acquire the JAVA source code, the Github library [37] was employed, and the FHE over AES scheme found in HELib was adopted. Real-world location data was drawn from the Open-StreetMap dataset [38], featuring a total of 62,556 real-world locations. For the simulation, the LBSP and LBS user were simulated within a single workstation using NS2 [39], while the CSP simulator was executed on another workstation employing CloudSim [40]. NS2 was chosen for constructing intricate network topologies and simulating query exchange. Notably, the LBSP served as the routing point, where each request from the LBS user and each response from LBSP had to pass through the CSP, introducing authentication steps and anonymization procedures that contributed to delays. In essence, the network models were extended to cater to the specific requirements of simulating the PPQ_FHE scheme within NS2, ensuring that all requests and responses traversed the CSP. These additional steps, including authentication and anonymization, imposed a processing overhead on the LBSP, affecting the overall performance of the scheme.

To evaluate the proposed HBfZkp model, we used the configuration given in table 1 as follows and evaluated entropy as well as the performance of the system. Further, we compare our results with existing well known approaches proposed in [48] and [56].

Table 2. Configuration Attributes

Attributes	Size
Social network server to mobile user (a)	64
Social network server to mobile user (b)	64
Mobile User to social network server	32
Mobile User to LBS	32
J (A)	64

From the experiments, we found that the entropy of our proposed HBfZkp is approximately 0.99 as shown in figure 3, which is much better than the existing both comparing approaches because of the decryption of single message which is most relevant.

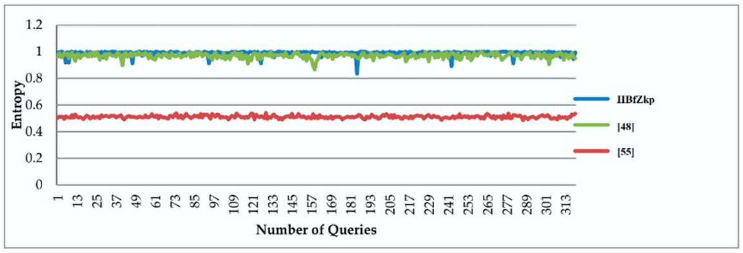

Figure 3. Entropy Comparison Of Proposed Hbfzkp Method With Existing Techniques.

Further we also evaluated the performance of overall systems. When comparing the performance entropy of HBfZkp to [48] and [55], it becomes evident that HBfZkp offers superior entropy. This improvement in entropy is primarily attributed to the utilization of the zero-knowledge proof algorithm in HBfZkp.

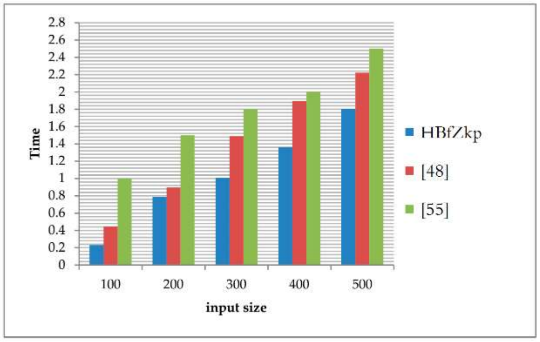

Figure 4. Performance Comparison Of Proposed Hbfzkp Method With Existing Techniques.

6. CONCLUSION

The paper explores the intricate landscape of privacy and security in Location-Based Services (LBS) LBS inherently face privacy and security challenges, particularly when user location data is involved. Protecting user data while maintaining service efficiency is a complex problem. Traditional methods such as Information Access Control, Mix Zones, k-anonymity, and dummy locations each have their limitations, making them susceptible to various forms of attacks and breaches. This paper introduces a compelling novel approach HBfZkp that is the Hybrid of Zero Knowledge Proofs (ZKPs) and Bloom Filters to address these critical concerns. This approach aims to asymptotically reduce information leakage and enhance security. Zero Knowledge Proofs provide a powerful tool for enhancing security. By ensuring that the LBS server only receives necessary information without revealing more, ZKPs offer a promising solution. On other hand, Bloom Filters play a vital role in optimizing runtime performance. When coupled with ZKPs, they contribute to a more comprehensive approach that addresses both efficiency and privacy. The paper presents experimental evaluations of the proposed approach to demonstrate its effectiveness and feasibility. These evaluations provide insights into the practical implementation of the hybrid solution. As technology evolves, continuous research in this field is essential. Future directions may involve refining the proposed approach by implementing in real environment, exploring new cryptographic techniques, and optimizing the integration of Bloom Filters for enhanced privacy and efficiency.

REFERENCES

[1]. N. Aggarwal, C. Gupta, and I. Sharma, "Fully Homomorphic symmetric scheme without bootstrapping," in Cloud Computing and Internet of Things (CCIOT), 2014 International Conference on, 2014, pp. 14-17.

[2] J. Alwen, M. Barbosa, P. Farshim, R. Gennaro, S. D. Gordon, S. Tessaro, et al., "On the relationship between functional encryption, obfuscation, and fully homomorphic encryption," in Cryptography and Coding, ed: Springer, 2013, pp. 65-84.

[3] V. Garg and M. Jhamb, "A Review of Wireless Sensor Network on Localization Techniques," International Journal of Engineering Trends and Technology (IJETT)-Volume4Isssue4-April, 2013.

[4] C. Gentry, J. Groth, Y. Ishai, C. Peikert, A. Sahai, and A. Smith, "Using fully homomorphic hybrid encryption to minimize non-interative zero-knowledge proofs," Journal of Cryptology, pp. 1-24, 2014.

[5] N. Smart, "Investigations of Fully Homomorphic Encryption (IFHE)," DTIC Document2015.

[6] Ashraf, Muhammad Usman. "A Survey on Data Security in Cloud Computing Using Blockchain: Challenges, Existing-State-Of-The-Art Methods, And Future Directions." Lahore Garrison University Research Journal of Computer Science and Information Technology 5, no. 3 (2021): 15-30.

[7] A. Leiva, N. Pavez, A. Beghelli, and R. Olivares, "A joint RSA algorithm for dynamic flexible optical networking," in Communications (LATINCOM), 2014 IEEE Latin-America Conference on, 2014, pp. 1-6.

[8] G. D. Sutter, J.-P. Deschamps, and J. L. Imaňa, "Modular multiplication and exponentiation architectures for fast RSA cryptosystem based on digit serial computation," Industrial Electronics, IEEE Transactions on, vol. 58, pp. 3101-3109, 2011.

[9] G. Asharov, A. Jain, A. López-Alt, E. Tromer, V. Vaikuntanathan, and D. Wichs, "Multiparty computation with low communication, computation and interaction via threshold FHE," in Advances in Cryptology–EUROCRYPT 2012, ed: Springer, 2012, pp. 483-501.

[10] Z. Brakerski and V. Vaikuntanathan, "Lattice-based FHE as secure as PKE," in Proceedings of the 5th conference on Innovations in theoretical computer science, 2014, pp. 1-12.

[11] S. Devadas, M. van Dijk, C. W. Fletcher, and

L. Ren, "Onion ORAM: A Constant Bandwidth and Constant Client Storage ORAM (without FHE or SWHE)," 2015.

[12] M. Naehrig, K. Lauter, and V. Vaikuntanathan, "Can homomorphic encryption be practical?," in Proceedings of the 3rd ACM workshop on Cloud computing security workshop, 2011, pp. 113-124.

[13] S. Mudda and S. Giordano, "Mobile P2P queries over temporal data," in Pervasive Computing and Communications Workshops (PERCOM Workshops), 2014 IEEE International Conference on, 2014, pp. 278-283.

[14] Alrahhal, Mohamad Shady, et al. "AES-route server model for location based services in road networks." International Journal Of Advanced Computer Science And Applications 8.8 (2017): 361-368.

[15] Ashraf, Muhammad Usman, et al. "IDP: A Privacy Provisioning Framework for TIP Attributes in Trusted Third Party-based Location-based Services Systems." , International Journal of Advanced Computer Science and Applications (IJACSA) 11.7 (2020): 604-617.

[16] Ashraf MU, Naeem M, Javed A, Ilyas I. H2E: A Privacy Provisioning Framework for Collaborative Filtering Recommender System. International Journal of Modern Education and Computer Science. 2019 Sep 1;11(9):1..

[17] L. Liu, L. Zhu, L. Lin, and Q. Wu, "Improvement of AODV Routing Protocol with QoS Support in Wireless Mesh Networks," Physics Procedia, vol. 25, pp. 1133-1140, 2012.

[18] K. Ren, "Exploiting Pairing-Based Zero Knowledge Proof (ZKP) for Tactical Network Authentication," DTIC Document2012.

[19] E. Ben-Sasson, A. Chiesa, D. Genkin, E. Tromer, and M. Virza, "SNARKs for C: Verifying program executions succinctly and in zero knowledge," in Advances in Cryptology–CRYPTO 2013, ed: Springer, 2013, pp. 90-108.

[20] S. Ranganathan, "Password Authentication for multicast host using zero knowledge Proof," International Journal of Electrical and Computer Engineering (IJECE), vol. 5, 2015.

[21] Ashraf MU, Qayyum R, Ejaz H. "State-of-the-art Challenges: Privacy Provisioning in TPP Location Based Services Systems.", International Journal of Advanced Research in Computer Science (IJARCS). 2019 Apr 20;10(2):68-75.

[22] A. M. R. Khan, T. Hashem, E. Tanin, and L. Kulik, "Location Oblivious Privacy Protection for Group Nearest Neighbor Queries," in Geographic Information Science, ed: Springer, 2014, pp. 301-317.

[23] W. Zhang, S. Liu, and Y. Xiaoyuan, "RLWE-Based Homomorphic Encryption and Private Information Retrieval," in Intelligent Networking and Collaborative Systems (INCoS), 2013 5th International Conference on, 2013, pp. 535-540.

[24] D. Boneh, A. Sahai, and B. Waters, "Functional encryption: a new vision for public-key cryptography," Communications of the ACM, vol. 55, pp. 56-64, 2012.

[25] A. J. Menezes, Elliptic curve public key cryptosystems vol. 234: Springer Science & Business Media, 2012.

[26] K. B. Swamy and K. K. Raju, "Multi-keyword Ranked Search over Encrypted Cloud Data Using RSA Algorithm," IJSEAT, vol. 3, pp. 307-311, 2015.

[27] S. Bai, R. Brent, and E. Thomé, "Root optimization of polynomials in the number field sieve," Mathematics of Computation, 2015.

[28] V. Grolmusz, "Separating the communication complexities of MOD m and MOD p circuits," in Foundations of Computer Science, 1992. Proceedings., 33rd Annual Symposium on, 1992, pp. 278-287.

[29] O. Chowdhury, D. Garg, L. Jia, and A. Datta, "Equivalence-based Security for Querying Encrypted Databases: Theory and Application to Privacy Policy Audits," in Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, 2015, pp. 1130-1143.

[30] A. Broder and M. Mitzenmacher, "Network applications of bloom filters: A survey," Internet mathematics, vol. 1, pp. 485-509, 2004.

[31] R. L. Moy, L.-S. Chen, and L. J. Kao, "Discrete Random Variables and Probability Distributions," in Study Guide for Statistics for Business and Financial Economics, ed: Springer, 2015, pp. 67-81.

[32] L. Bunimovich, I. Cornfeld, R. Dobrushin, N. Maslova, Y. B. Pesin, A. Vershik, et al., Dynamical Systems II: Ergodic Theory with Applications to Dynamical Systems and Statistical Mechanics vol. 2: Springer Science

& Business Media, 2013.

[33] M. Youssef, V. Atluri, and N. R. Adam, Preserving mobile customer privacy: An access control system for moving objects and custom proles. s.l. : In Proc. MDM 2005.

[34] Mobimix, B. Palanisamy and L. Liu, Protecting location privacy with mix-zones over road networks. s.l. : In Proc. ICDE 2011.

[35] B. Bamba, L. Liu, P. Pesti, and T. Wang, Supporting anonymous location queries in mobile environments with PrivacyGrid. s.l. : In Proc. WWW 2008.

[36] C.-Y. Chow, M. F. Mokbel, and W. G. Aref, "Casper*: Query processing for location services without compromising privacy," ACM Trans. Database Syst., vol. 34, no. 4, 2009.

[37] P. Shankar, V. Ganapathy and L. Iftode, Privately querying location-based services with SybilQuery. s.l. : In Proc. Ubicomp 2009.

[38] O. Han, H. Zhao, Z. Ma, K. Zhang, and H. Pan, Protecting Location Privacy Based on Historical Users over Road Networks .. s.l. : In Proc. WASA 2014.

[39] Ashraf MU, Arif S, Basit A, Khan MS. Provisioning quality of service for multimedia applications in cloud computing. Int. J. Inf. Technol. Comput. Sci.(IJITCS). 2018;10(5):40-7.

[40] B. Yao, F. Li, and X. Xiao, Secure nearest neighbor revisited. s.l. : In Proc. ICDE 2013.

[41] W. K. Wong, D. W. Cheung, B. Kao, and N. Mamoulis, Secure kNN computation on encrypted databases.s.l. : In Proc. SIGMOD 2009.

[42] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K. L. Tan, Private queries in location-based services: Anonymizers are not necessary. s.l. : In Proc. ACM SIGMOD 2008.

[43] S. Papadopoulos, S. Bakiras, D. Papadias, Nearest neighbor search with strong location privacy. s.l. : In Proc. VLDB 2010.

[44] R. Paulet, M. G. Kaosar, X. Yi, and E. Bertino, "Privacy-preserving and content-protecting location based queries," Knowledge and Data Engineering, IEEE Transactions on, vol. 26, pp. 1200-1210, 2014.

[45] Z. Zhu and G. Cao, "Applaus: A privacy-preserving location proof updating system for location-based services," in INFOCOM, 2011 Proceedings IEEE, 2011, pp. 1889-1897.

[46] A. Pingley, W. Yu, N. Zhang, X. Fu, and W. Zhao, "A context-aware scheme for privacy-preserving location-based services," Computer Networks, vol. 56, pp. 2551-2568, 2012.

[47] C. Dong, L. Chen, and Z. Wen, "When private set intersection meets big data: an efficient and scalable protocol," in Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security, 2013, pp. 789-800.

[48] N. Shen, J. Yang, K. Yuan, C. Fu and C. Jia, "An efficient and privacy-preserving location sharing mechanism", Computer Standards & Interfaces, vol. 44, pp. 102-109, 2015.

[49] X. Zhu, D. Hu, Z. Hou and L. Ding, "A location privacy preserving solution to resist passive and active attacks in VANET", China Communications, vol. 11, no. 9, pp. 60-67, 2014.

[50] M. Xiao, J. Wu and L. Huang, "Home-Based Zero-Knowledge Multi-Copy Routing in Mobile Social Networks", IEEE Trans. Parallel Distrib. Syst., vol. 26, no. 5, pp. 1238-1250, 2015.

[51] Y. Zhu, L. Ma and J. Zhang, "An enhanced Kerberos protocol with non-interactive zero-knowledge proof", Security and Communication Networks, vol. 8, no. 6, pp. 1108-1117, 2014.

[52] P. Jagwani and S. Kaushik, "Defending Location Privacy Using Zero Knowledge Proof Concept in Location Based Services," pp. 368-371, 2012.

[53] P. Kotzanikolaou, E. Magkos, N. Petrakos, C. Douligeris, and V. Chrissikopoulos, "Fair anonymous authentication for location based services," In Data Privacy Management and Autonomous Spontaneous Security. Heidelberg: Springer, 2013, pp. 1-14.

[54] V. Mainanwal, M. Gupta, and S. K. Upadhayay, "Zero Knowledge Protocol with RSA Cryptography Algorithm for Authentication in Web Browser Login System (Z-RSA)," pp. 776-780, 2015.

[55] S. Geol Choi, J. Katz, D. Schr¨oder, A. Yerukhimovich, and H-S. Zhou, "(efficient) universally composable oblivious transfer using a minimal number of stateless tokens," presented at the 11th Theory of Cryptography Conference (TCC), In: Lindell, 2014.

[56] V. Gupta, T. S. Vineeth, and V. Aggarwal, "Make Your Query Anonymous With Oblivious Transfer," in Proceedings of the Sixth International Conference on Computer and Communication Technology 2015, 2015, pp. 345-349.

[57] C. Cachin, C. Crepeau, J. Marcil and G. Savvides, "Information-Theoretic Interactive Hashing and Oblivious Transfer to a Storage-Bounded Receiver", IEEE Trans. Inform. Theory, vol. 61, no. 10, pp. 5623-5635, 2015.

[58] G. Asharov, Y. Lindell, T. Schneider, M. Zohner: More Efficient Oblivious Transfer Extensions with Security for Malicious Adversaries. EUROCRYPT (1) 2015: 673-701.

[59] H. Li, X. Cheng, K. Li, and Z. Tian, "Efficient Customized Privacy Preserving Friend Discovery in Mobile Social Networks," in Distributed Computing Systems (ICDCS), 2015 IEEE 35th International Conference on, 2015, pp. 225-234.

[60] L. Calderoni, P. Palmieri, and D. Maio, "Location privacy without mutual trust: The spatial Bloom filter," Computer Communications, vol. 68, pp. 4-16, 2015.

[61] P. Palmieri, L. Calderoni, D. Maio, Spatial bloom filters: enabling privacy in location-aware applications, in: Lecture Notes in Computer Science, vol. 8957, Springer, 2015, pp. 16-36.

[62] M. Ahmadi and R. Pourian, "A Bloom Filter with the Integrated Hash Table Using an Additional Hashing Function," Network Protocols and Algorithms, vol. 7, p. 24, 2015.

[63] Google Books, "Patent US6061789 - Secure anonymous information exchange in a network", 2015. [Online]. Available: https://www.google.com/patents/US6061789. [Accessed: 30- Dec- 2015].