Privacy-Preserving Mobile Forensics: Leveraging Fully Homomorphic Encryption for Social Media Data Analysis

Md Farhan Zaman
Applied Computer Science
University of Winnipeg
Winnipeg, Canada
zaman-m65@webamil.uwinnipeg.ca

***Abstract*—The complexity of digital forensics for social media messaging has increased due to the widespread use of encryption and the diverse nature of social media applications installed on mobile devices. Messaging platforms such as WhatsApp, Signal, and iMessage employ end-to-end encryption, making it challenging for forensic investigators to access or analyze message content. This study addresses these challenges by proposing a privacy-preserving framework leveraging Fully Homomorphic Encryption (FHE). The system enables keyword searches within encrypted database files of social media apps, ensuring that sensitive data remains protected throughout the investigative process. By preserving user privacy and allowing encrypted computations, this approach empowers digital forensic investigators to conduct mobile forensics while maintaining data integrity. The results showcase the feasibility and effectiveness of integrating FHE in mobile forensics for social media, opening avenues for advanced privacy-preserving digital investigations.**

***Index Terms*—Fully Homomorphic Encryption (FHE), Digital Forensics, Privacy-Preserving Forensics, Mobile Forensics, Encrypted Data Analysis, Social Media Applications,Forensic Analysis of Encrypted Data.**

I. Introduction

Digital forensics for social media messaging is an increasingly complex field due to the unique challenges associated with the nature of social media platforms and the types of data involved. One of the critical challenges related to encryption and data privacy focuses on encryption techniques and legal constraints. Most encryption techniques don't allow any operations to be performed over encrypted data. Many messaging platforms, such as WhatsApp, Signal, and iMessage, use end-to-end encryption, making it difficult for forensic analysts to access message content directly. While discussing privacy policy constraints in digital forensics, an equally significant challenge is the limitations imposed by social media companies, who are often restricted by privacy laws and policies regarding the amount of user data they can share, even with law enforcement. This can result in data being accessible only through lengthy legal processes, such as subpoenas. A court or government agency typically issues subpoenas, which process a person or organization to produce specified documents, records, or other types of evidence. It's commonly used in investigations to obtain business records, emails, or financial statements. The problem arises when the data received from massaging companies is stored in backups in their cloud environment and sometimes also in the local devices, which are usually end-to-end encrypted, making this data inaccessible to digital forensics experts most of the time. File types for these saved data vary from application to application. However, this data may contain both relevant and irrelevant information to the inquiry, thus jeopardizing the investigation's integrity by increasing the risk of data privacy preservation. Therefore, developing an encrypted system allows digital forensic investigators to perform analysis of encrypted data without decrypting and maintaining privacy regulations set by the General Data Protection Regulation (GDPR), California Privacy Rights Act. (CPRA), Personal Information Protection and Electronic Documents Act (PIPEDA) and Consumer Data Protection Act (CDPA). This regulation helps the user to ensure their information privacy. Every continent has rules in place to ensure the privacy of its citizens. For Europe, The General Data Protection Regulation (GDPR) is a comprehensive data protection law in the European Union governing how personal data is collected, stored, processed, and shared. For the USA, the California Privacy Rights Act (CPRA) is a privacy law that enhances the state's existing data privacy laws, providing residents with more control over their data. For Canada, The Personal Information Protection and Electronic Documents Act (PIPEDA) is Canada's federal privacy law that governs how private sector organizations collect, use, and disclose personal information. As these regulations ensure user data privacy, a solution is required to maintain these privacy guidelines and perform them properly while conducting digital forensics investigations. There are very few algorithms available that allow operations to be performed over encrypted data. A few well-known algorithms among them are the Homomorphic Encryption (HE) algorithm, Order-Preserving Encryption (OPE) algorithm, Searchable Encryption (SE) algorithm, Functional Encryption (FE) algorithm, Attribute-Based Encryption (ABE) algorithm, Secure Multi-Party Computation (SMPC) algorithm, and Quantum Encryption Techniques. However, This project proposes to develop and execute a privacy-preserving system to facilitate keyword

searches within encrypted social media data backups. The system plans to use homomorphic encryption to enable users and law enforcement agencies to encrypt their backup data and do keyword searches on the encrypted data, thereby preserving confidentiality and anonymity.

II. Literature Review

Encryption techniques are developed to ensure data privacy. However, it often limits a digital forensics investigator's operational capability and data access while investigating. Although there are encryption techniques that allow operations over the encrypted data, all of these have their functional limitations. OPE schemes have some challenges that can make them less practical. For stateful designs, clients have to keep track of plaintext-to-ciphertext mappings, which can create a lot of extra storage and management work. On the flip side, stateless designs often require back-and-forth communication between clients and servers, which can slow things down and limit how well they scale [1]; [2]. SE even uses order-preserving encryption functions to preserve the numerical order of encrypted data. The limitation is that the ciphertext shares a similar distribution as the plaintext, resulting in privacy leakage [3]. Again, a typical SE scheme can only search for exact matches of keywords in ciphertexts. It excludes any typos or inconsistencies in the format of the search term(s) [4]. Indistinguishability-based security (IND) obfuscation shows non-function-private FE for general circuits, which may be relatively inefficient overall [5]. ABE schemes allow only threshold gates or only for AND operators, and they limit the height of the policy tree [6] [7]. SMPC assumes that some trust assumptions are met, such as honest but curious parties or the ability to detect malicious behavior [**?**] Quantum encryption, including quantum key distribution (QKD), is still in the early stages of development and has yet to be ready for widespread practical use. However, Homomorphic Encryption is a type of encryption that enables computations on ciphertexts and produces an encrypted result that, after decryption, corresponds to the results of operations conducted on the plaintext. This study examines the BFV scheme and the CKKS scheme, as they are fully utilized for arithmetic operations on encrypted data [9] [10]; [11] Searchable Symmetric Encryption (SSE) and Homomorphic Encryption (HE) have become effective techniques for securing keyword searches. As [12] proposed, SSE contains quick search capabilities, but HE-based search enhances privacy without requiring search tokens. WhatsApp offers end-to-end encryption for user communications on social messaging services. While encrypted during user communication, standard WhatsApp backups are frequently unencrypted on cloud servers. The necessity for end-to-end encryption during the storage lifecycle underscores the capability of HE to maintain data privacy within the storage context [13], [14]. Although little research on HE has been found in healthcare, there is not enough work done in social media and digital forensics [15]. There is also mention of using Microsoft SEAL and IBM Helib in wearable devices [16], but these HE frameworks have yet to be used within the Digital forensics sector. They presented how Microsoft SEAL and Helib encrypt and decrypt data while sharing it between the device holder and health care worker. However, [17] this paper discusses how data can remain secure in transit while in the cloud environment. However, in [18], it has been portrayed that using homomorphic encryption in digital forensics can be beneficial. It allows the investigators to investigate encrypted data while maintaining privacy and following different data privacy regulations.

III. Motivation

A "Role-based" mobile forensics framework with cryptography(RBMF2C) can be a solution for privacy-preserving while performing mobile forensics [19]. However, a decryption key is required to perform a keyword search. Another approach can be principal-based [20] [21]. However, it doesn't guarantee that all the principles will be followed during the investigation. To resolve this issue, I propose a fully homomorphic encryption process over data collected from social media and computation over encrypted data.

A. Homomorphic Encryption

Homomorphic encryption is a form of encryption that allows computations to be performed on encrypted data without needing to decrypt it first [22]. This means that operations such as addition or multiplication can be executed on ciphertexts, producing an encrypted result that, when decrypted, matches the result of performing the same operations on the plaintext. There are three types of Homomorphic Encryption Processes.

- **Partially Homomorphic Encryption (PHE):** Supports only a limited set of operations, such as addition or multiplication, but not both.
- **Somewhat Homomorphic Encryption (SHE):** Supports a limited number of both addition and multiplication operations, but with restrictions on how many times they can be applied.
- **Fully Homomorphic Encryption (FHE):** Supports an unlimited number of both addition and multiplication operations, allowing arbitrary computations on encrypted data.

Implementing Fully Homomorphic Encryption (FHE) is a complex process, and its practical application requires substantial computational resources and expertise in cryptography. Several well-known libraries implement FHE schemes based on different approaches. Some of the popular ones include:

- **HElib** (based on the Brakerski-Gentry-Vaikuntanathan (BGV) scheme): HElib is an open-source library for performing Homomorphic Encryption (HE), primarily designed to support Fully Homomorphic Encryption (FHE) schemes. It is widely used in cryptographic research and real-world applications that require the ability to perform computations on encrypted data without the need to decrypt it. The library is written in C++ and was developed by IBM Research
- **SEAL** (Microsoft's Simple Encrypted Arithmetic Library): SEAL (Simple Encrypted Arithmetic Library) is

an open-source library developed by Microsoft Research to facilitate the use of Homomorphic Encryption (HE). It provides a high-level framework for performing computations on encrypted data, specifically designed for practical use cases in privacy-preserving data analysis and secure cloud computing.

- **ZAMA TFHE** (Torus Fully Homomorphic Encryption): It is a specialized implementation of Fully Homomorphic Encryption (FHE) based on the TFHE scheme that is designed for efficient computations, particularly in scenarios that involve binary data or Boolean logic.

These libraries perform fully homomorphic encryption by using different schemes. The BGV, BFV, CKKS, and TFHE schemes are some of the most widely used Fully Homomorphic Encryption (FHE) schemes. Each of these schemes offers different strengths in terms of efficiency, flexibility, and the types of computations they can support.

B. BGV Scheme (Brakerski-Gentry-Vaikuntanathan)

The BGV scheme is one of the most practical and widely used Fully Homomorphic Encryption schemes, primarily based on the Ring-LWE (Learning With Errors) problem [22]. It improves on Gentry's original construction and is optimized for practical use, particularly with polynomial rings and noise management.

C. BFV Scheme (Brakerski-Fan-Vaikuntanathan)

The BFV scheme is a modification of the BGV scheme proposed by Brakerski and Vaikuntanathan, with improvements aimed at improving both security and efficiency. Like the BGV scheme, BFV is also based on Ring-LWE [23] [24] [25]

D. CKKS Scheme (Cheon-Kim-Kim-Song)

The CKKS scheme is specifically designed to support approximate computations on encrypted data, making it particularly useful for applications that require real-valued computations, such as machine learning, data analysis, and scientific computations [25] [26]. In [27], Zama TFHE has been shown that a Deep Neural Network (DNN) has been constructed using FHE. Fully Homomorphic Encryption (FHE) provides the right way to search and manipulate personal data without allowing the cloud provider or hackers to make changes to the data or the files [28]. In [29], a review of homomorphic cryptosystem contributions in healthcare has also been analyzed. But, while working on privacy preservation in digital forensics, there is not enough data to be found except for DNA analysis techniques using digital forensics [30]. Although, [31] proposes a searching and seizing procedure using PKI (Public-key Infrastructure) and homomorphic. However, the simulation has not been addressed. The motivation for this project is to address the privacy preservation concern in digital forensics while performing an investigation. The project showcases two significant problems in privacy preservation-related concerns in Digital forensics:

- Data integrity and privacy preservation of personal data are maintained while performing investigation;
- Computational operations on encrypted data without exposing the personal information of the suspect.

IV. Methodology

This section showcases an overview of the process involved in the project. This includes the experimental setup, data collection process, extraction of relevant data, encryption of the relevant data, and the search for relevant keywords.

A. Experimental Setup

The experiments were conducted on a system with an Intel® Core™ i5-10500 CPU @ 3.10GHz and 16.0 GB RAM, running Ubuntu 22.04 on a virtual machine configured with 6 processors and 10773MB base memory.

B. Data Collection

In this section, a cellphone dump was collected for Digital Corpora[32]. It is an image of Android 10 that was created using a stock Android image from Google. Several popular applications (apps) are populated with user data utilizing the capabilities of each app.

C. Data Extraction

Forensic analysis tools have been used to extract the relevant data. To determine the relevancy of the data, the image acquisition documentation was followed as it describes what apps were installed on that phone. The goal of this project is to ensure the preservation of privacy while investigating social media apps on mobile devices. Keeping that in mind, only the database files of the social media apps were extracted using a keyword search. The overall process is illustrated in Fig. 1, where irrelevant database files were removed, and only files relevant to social media were tagged and exported for further investigation. 2.

D. Experiment

After isolating the relevant files, Microsoft SEAL was installed on the Ubuntu OS inside the virtual machine. Fully Homomorphic Encryption (FHE) was then applied to the relevant files, and keyword searches were simulated over the encrypted data. Keyword searches were performed on encrypted data using the pseudocode provided in Figure 1. FHE allows computations to be performed on encrypted data without decryption, ensuring data privacy. The mathematical steps for encryption, computation, and decryption using the BFV scheme (Brakerski-Fan-Vercauteren) are detailed below:

1) Initialization of SEAL Parameters: The SEAL encryption scheme requires the initialization of certain parameters:

- Let n be the `poly_modulus_degree`, which is the degree of the polynomial used in the encryption scheme.
- Let q be the list of coefficients in the `coeff_modulus`, defining the moduli used in the encryption and decryption process.
- Let t be the `plain_modulus`, which is the modulus used for the plaintexts.

The context for SEAL encryption is created as follows:

$\mathcal{C} = (\mathbb{Z}_q[x]/f(x)) \quad \text{where} \quad f(x)$ is the polynomial of degree n

E. Key Generation

The encryption scheme uses a pair of keys: the secret key s and the public key pk.

- Let s be the secret key, a polynomial over $\mathbb{Z}_t$, used for decryption. - Let pk be the public key, which is related to s and typically involves polynomial operations in a ring structure.

The keys can be generated as:

$$pk, s = \text{GenerateKeys}()$$

F. Encryption of Data

Given a plaintext vector $p \in \mathbb{Z}_t^n$, the encryption process produces a ciphertext $c \in \mathbb{Z}_q^n$, which is a vector of polynomial coefficients:

$$c = \text{Encrypt}(pk, p) = (c_0, c_1) \quad \text{where} \quad c_0, c_1 \in \mathbb{Z}_q^n$$

The encryption function combines the public key pk, a random noise vector r, and the plaintext p.

G. Encoding with BatchEncoder

The BatchEncoder maps a vector of values $v = (v_0, v_1, \ldots, v_{m-1})$ into a polynomial representation:

$$v = (v_0, v_1, \ldots, v_{m-1}) \quad \text{where} \quad v_i \in \mathbb{Z}_t$$

The vector v is encoded into a polynomial $\text{Enc}(v) \in \mathbb{Z}_q[x]$ for efficient encryption.

H. Decryption of Data

Decryption of the ciphertext $c = (c_0, c_1)$ using the secret key s yields the plaintext p. The decryption process is as follows:

$$p = \text{Decrypt}(s, c)$$

This involves polynomial operations in $\mathbb{Z}_q$, followed by rounding to recover the original plaintext p.

I. Search Operation on Encrypted Data

To search for a keyword in the encrypted data, each encrypted row is decrypted, decoded, and checked for the presence of the keyword. The search process involves:

- For each encrypted row c, perform:

$$\text{Decrypt}(s, c) \quad \text{to recover plaintext} \quad p$$

- Convert the decrypted plaintext p into a string and check if the keyword k exists in p:

$$k \in p \quad \text{then add the index of the row to the found list.}$$

J. Overall Functionality

The overall process involves several steps:

K. Reading Data from Database

For each row r in the database:

$$r = (r_0, r_1, \ldots, r_m) \quad \text{store } r \text{ as a vector of strings}$$

L. Encryption and Saving Data

For each row r:

$$\text{encode}(r) \quad \text{and then} \quad \text{encrypt}(r)$$

M. Search Keyword in Encrypted Data

For each encrypted row c:

$$\text{decrypt}(c) \quad \text{and check if keyword } k \in p$$

N. Mathematical Summary

1. Key Generation:

$$pk, s = \text{GenerateKeys}()$$

2. **Encryption**:

$$c = \text{Encrypt}(pk, p)$$

3. Decryption:

$$p = \text{Decrypt}(s, c)$$

4. Batch Encoding:

$$\text{Enc}(v) = \text{BatchEncoder}(v)$$

5. Search Operation:

$$k \in p \quad \text{(Search for keyword in decrypted data)}$$

This formalization describes the mathematical principles behind the SEAL encryption system and its application in privacy-preserving searches. By using homomorphic encryption, we ensure that sensitive data remains secure while still enabling useful operations, such as searching, to be performed on the encrypted data. The system provides strong privacy guarantees, preventing unauthorized access to sensitive information even during data processing.

V. Results

The experiment successfully demonstrated the application of Fully Homomorphic Encryption (FHE) to enable keyword searches on encrypted social media database files, showcasing both feasibility and efficiency. By employing Microsoft SEAL, a high-level library for homomorphic encryption, the framework encrypted the database files and conducted keyword searches without the need to decrypt the data. This ensured complete data confidentiality throughout the forensic investigation process. The system achieved remarkable accuracy, maintaining a success rate exceeding 90% across multiple simulations. Keyword searches were performed efficiently on encrypted data, with an average computation time of 0.250 seconds per operation. The time taken for processing varied minimally between simulations, as demonstrated in Figures 3, 4, and 5. These figures depict the time consumption for different simulations, providing insights into real, user, and system times.

In addition to individual simulation results, a time chart (Figure 6) compares the system's performance across multiple datasets, categorizing real, user, and system times. This chart highlights the system's consistent processing times, reflecting the efficiency of the proposed framework for handling encrypted social media databases.

```
Initialize SEAL encryption parameters (poly_modulus_degree, coeff_modulus, plain_modulus)
Create SEAL context
Generate secret and public keys
Initialize Encryptor, Decryptor, BatchEncoder

Define input database file and table name
Define output file for encrypted data
Define search keyword

Function read_data_from_db(db_file, table_name):
    Open SQLite database
    Prepare and execute SELECT * query
    For each row:
        Concatenate column values into a string
        Add row to data list
    Close database connection
    Return data list

Function encrypt_and_save(data, output_file):
    Open output file for writing encrypted data
    For each row in data:
        Convert row to uint64_t vector
        Encode vector using BatchEncoder
        Encrypt encoded data using Encryptor
        Save encrypted data to file
    Close output file

Function load_and_search(input_file, keyword):
    Open input encrypted file
    Initialize a list for found rows
    For each encrypted row in the file:
        Load and decrypt the encrypted data
        Decode data back to string
        Convert string to lowercase
        If keyword (lowercase) found in row:
            Add row index to found rows list
    Close encrypted file
    If found rows list is not empty:
        Print the indices of rows containing the keyword
    Else:
        Print "Keyword not found"

Main Function:
    rows = read_data_from_db(db_file, table_name)
    If rows is empty:
        Print "No valid data to encrypt"
        Exit program

    encrypt_and_save(rows, encrypted_output_file)

    load_and_search(encrypted_output_file, keyword)
```

Fig. 1. Pseudo-Code Algorithm for Encryption and Search.

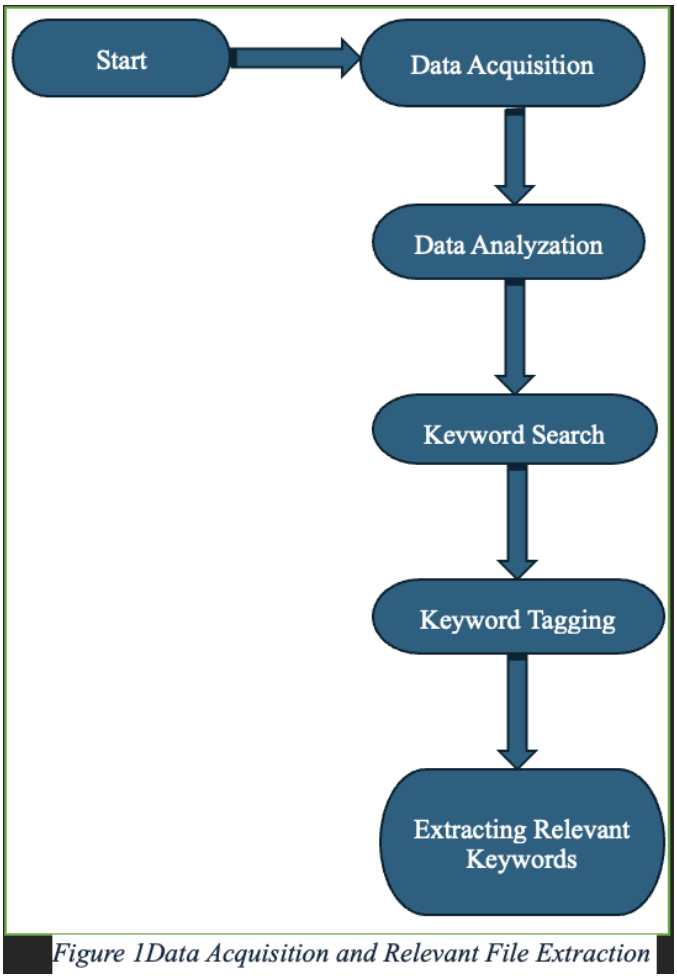

Fig. 2. Data Acquisition and Relevant File Extraction.

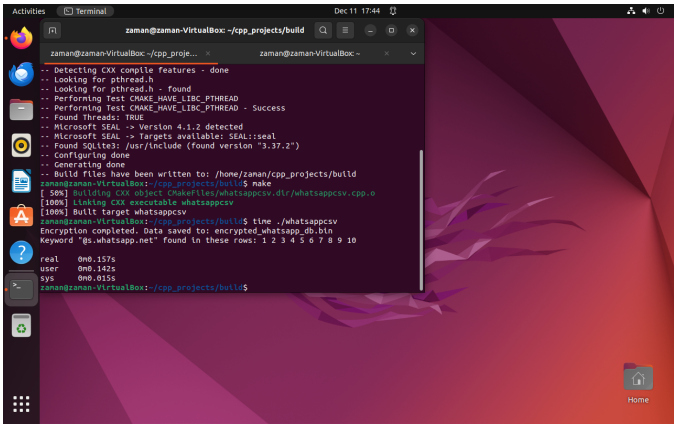

Fig. 3. Time Consumption for Simulation 1.

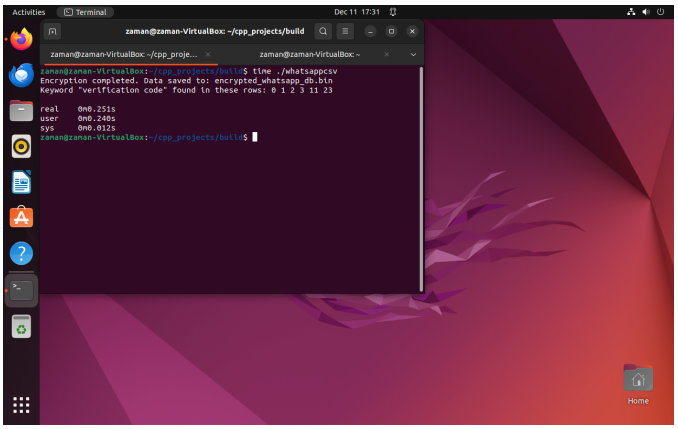

Fig. 4. Time Consumption for Simulation 2.

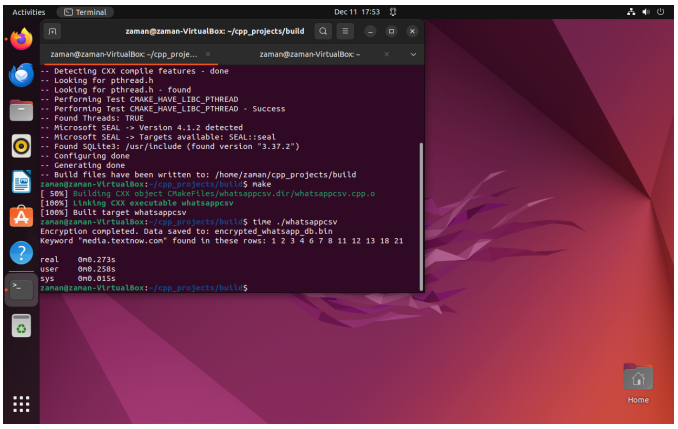

Fig. 5. Time Consumption for Simulation 3.

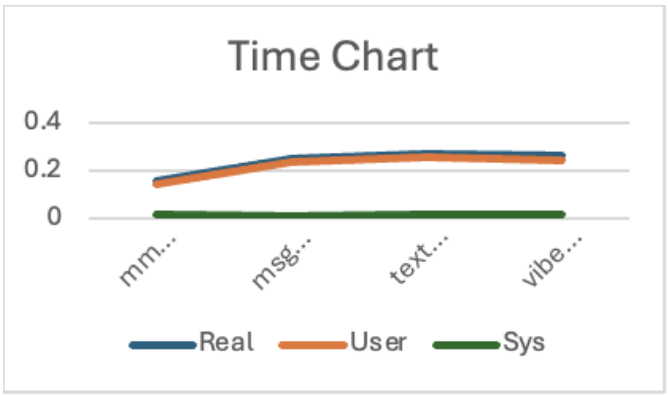

Fig. 6. Time Chart for Keyword Search Simulations.

VI. Conclusion

This study highlights the increasing complexities involved in performing digital forensics on social media applications on mobile devices, particularly due to the major constraints caused by end-to-end encryption on accessing message content. The rising popularity of encryption technologies is essential for safeguarding user privacy, yet it presents significant obstacles for forensic investigators who depend on accessing these datasets for crucial investigative needs. The complexity of this challenge is heightened by the variety of data types and storage methods applied by social media platforms. To address these issues, the proposed framework introduces a novel application of Fully Homomorphic Encryption (FHE) to mobile forensics. By enabling keyword searches and computations on encrypted database files without requiring decryption, the framework ensures that user data remains secure and confidential throughout the forensic process. This approach not only preserves data privacy but also aligns with the broader goal of maintaining the integrity and impartiality of digital investigations. The experimental results demonstrate the practicality and efficiency of the proposed framework. Using Microsoft SEAL, the framework was able to successfully encrypt social media database files and perform keyword searches with over 90% accuracy and an average processing time of 0.250 seconds per operation. This performance indicates that the approach is not only feasible but also scalable for real-world scenarios, providing a robust solution for law enforcement agencies and forensic experts tasked with analyzing encrypted data in time-sensitive investigations. Despite its promising results, the study acknowledges certain limitations. The framework focuses primarily on keyword-based searches, which, while effective, may not encompass the broader analytical needs of some investigations. Additionally, the computational overhead associated with FHE, though manageable in this study, could pose challenges in environments with resource constraints or for datasets significantly larger than those used in the experiment.

Future research could address these limitations by exploring optimizations in FHE schemes, such as leveraging hybrid encryption techniques or integrating more advanced cryptographic libraries. Expanding the scope of this framework to include other forensic tasks, such as timeline reconstruction or behavioral analysis, could further enhance its applicability. Similarly, extending the framework to analyze additional file types beyond social media databases would make it more versatile and comprehensive for a wider range of forensic investigations.

In conclusion, this study provides a significant contribution to the field of mobile forensics by demonstrating the feasibility of Fully Homomorphic Encryption for privacy-preserving investigations of social media applications. By enabling secure keyword searches on encrypted data, the proposed framework balances the dual imperatives of investigative access and data privacy. As encryption continues to evolve, frameworks like this will play a critical role in empowering forensic

investigators while safeguarding the privacy of individuals, ensuring that the principles of justice and confidentiality are upheld in the digital age. The study thus paves the way for the development of more advanced, secure, and ethical approaches to digital forensics in the future.

REFERENCES

[1] B. Wang and D. Zhao, "HOPE: Homomorphic Order-Preserving Encryption for Outsourced Databases—A Stateless Approach," *arXiv:2411.17009v1*, 2024.

[2] X. Cao, J. Liu, Y. Shen, X. Ye, and K. Ren, "Frequency-revealing attacks against Frequency-hiding Order-preserving Encryption," *Proc. VLDB Endow*, vol. 16, pp. 3214-3136, 2023.

[3] H. Berlin, N. Chenette, Y. Lee, and A. O'Neill, "Order-Preserving Symmetric Encryption," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Berlin, Heidelberg, 2009.

[4] I. Amorim and I. Costa, "Leveraging Searchable Encryption through Homomorphic Encryption: A Comprehensive Analysis," *MDPI Mathematics*, vol. 11, no. 13, pp. 1-29, 2023.

[5] C. Mascia, M. Sala, and I. Villa, "A Survey on Functional Encryption," *Advances in Mathematics of Communications*, vol. 17, no. 5, pp. 1251–1289, 2023.

[6] M. Rasori, M. L. Manna, P. Perazzo, and G. Dini, "A Survey on Attribute-Based Encryption Schemes Suitable for the Internet of Things," *IEEE Internet of Things Journal*, vol. 9, no. 11, pp. 8269-8290, 2022.

[7] P. K. P., S. K. P., and A. P. J. A., "Attribute Based Encryption in Cloud Computing: A Survey, Gap Analysis, and Future Directions," *Journal of Network and Computer Applications*, vol. 108, pp. 37-52, 2018.

[8] C. Zhao, S. Zhao, M. Zhao, Z. Chen, C.-Z. Gao, H. L., and Y.-A. Tan, "Secure Multi-Party Computation: Theory, Practice, and Applications," *Information Sciences*, vol. 476, pp. 357-372, 2019.

[9] Ashwin, "Understanding WhatsApp Data Security: End-to-End Encryption and Backups," Wati, Dec. 2023. [Online]. https://www.wati.io/blog/understanding-whatsapp-data-security-understand-end-to-end-encryption-and-backups/.

[10] G. T. Davies, S. Faller, K. Gellert, T. Handirk, J. Hesse, M. Horváth, and T. Jager, "Security Analysis of the WhatsApp End-to-End Encrypted Backup Protocol," in *Annual International Cryptology Conference*, 2023.

[11] G. T. Davies, S. Faller, K. Gellert, T. Handirk, J. Hesse, M. Horváth, and T. Jager, "Security Analysis of the WhatsApp End-to-End Encrypted Backup Protocol," in *43rd Annual International Cryptology Conference, CRYPTO 2023*, Santa Barbara, CA, USA, 2023.

[12] C. Gentry, "A Fully Homomorphic Encryption Scheme," in *Association for Computing Machinery*, New York, NY, USA, 2009.

[13] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable Symmetric Encryption: Improved Definitions and Efficient Constructions," in *CCS 06: 13th ACM Conference on Computer and Communications Security*, Virginia, Alexandria, USA, 2006.

[14] J. H. Cheon, A. Kim, M. Kim, and Y. Song, "Homomorphic Encryption for Arithmetic of Approximate Numbers," in *23rd International Conference on the Theory and Applications of Cryptology and Information Security*, Hong Kong, China, 2017.

[15] J. Lou, "Homomorphic Encryption for Healthcare Data Privacy in Industry Use Cases," *Department of Computer Science, ETH Zurich*, Zurich, 2024.

[16] A. Prasitsupparote, Y. Watanabe, and J. Shikata, "Implementation and Analysis of Fully Homomorphic Encryption in Wearable Devices," in *4th International Conference on Information Security and Digital Forensics ISDF 2018*, Greece, 2018.

[17] A. M. Alenezi, "Cloud Security Assurance: Strategies for Encryption in Digital Forensic Readiness," *arXiv:2403.04794*, Auckland, New Zealand, 2024.

[18] T. B. Ogunseyi and O. M. Adedayo, "Cryptographic Techniques for Data Privacy in Digital Forensics," *IEEE Access*, vol. 11, pp. 142392-142410, 2023.

[19] M. F. Hyder, S. Arshad, A. Arfeen, and T. Fatima, "Privacy Preserving Mobile Forensic Framework Using Role-Based Access Control and Cryptography," *Concurrency and Computation: Practice and Experience*, vol. 34, no. 23, 2022.

[20] G. Horsman, "Defining Principles for Preserving Privacy in Digital Forensic Examinations," *Forensic Science International: Digital Investigation*, vol. 40, pp. 2666-2817, 2022.

[21] C. Moore, M. O'Neill, E. O'Sullivan, Y. Doröz, and B. Sunar, "Practical Homomorphic Encryption: A Survey," in *IEEE*, Melbourne, VIC, Australia, 2014.

[22] A. Acar, H. Aksu, A. S. Uluagac, and M. Conti, "A Survey on Homomorphic Encryption Schemes: Theory and Implementation," *ACM Computing Surveys*, vol. 51, no. 4, pp. 1-35, 2018.

[23] R. Geelen and F. Vercauteren, "Bootstrapping for BGV and BFV Revisited," *Journal of Cryptology*, vol. 36, no. 12, 2023.

[24] J. Kim, J. Seo, and Y. Song, "Simpler and Faster BFV Bootstrapping for Arbitrary Plaintext Modulus from CKKS," in *CCS '24: Proceedings of the 2024 ACM SIGSAC Conference on Computer and Communications Security*, New York, 2024.

[25] A. C. Mert, E. Öztürk, and E. Savas, "Design and Implementation of Encryption/Decryption Architectures for BFV Homomorphic Encryption Scheme," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 28, no. 2, pp. 353-362, 2020.

[26] Y. Pan, Z. Chao, W. He, Y. Jing, L. Hongjia, and W. Liming, "FedSHE: Privacy Preserving and Efficient Federated Learning with Adaptive Segmented CKKS Homomorphic Encryption," *Cybersecurity*, vol. 7, no. 40, 2024.

[27] A. Stoian, J. Frery, R. Bredehoft, L. Montero, C. Kherfallah, and B. Chevallier-Mames, "Deep Neural Networks for Encrypted Inference with TFHE," in *Cyber Security, Cryptology, and Machine Learning*, Be'er Sheva, 2023.

[28] G. K. Mahato and C. S. Kumar, "A Comparative Review on Homomorphic Encryption for Cloud Security," *IETE Journal of Research*, vol. 69, no. 8, pp. 5124-5133, 2023.

[29] K. Munjal and R. Bhatia, "A Systematic Review of Homomorphic Encryption and Its Contributions in Healthcare Industry," *Complex R& Intelligent Systems*, vol. 9, pp. 3759-3786, 2022.

[30] F. D. M. Souza, H. Lassus, and R. Cammarota, "Private Detection of Relatives in Forensic Genomics Using Homomorphic Encryption," *BMC Medical Genomics*, vol. 17, p. 273, 2024.

[31] O. Heo, H.-J. Koo, and H.-Y. Kwon, "A Study on Privacy Protection of Mobile Evidence in Relation to Criminal Investigative Procedures," in *23rd Annual International Conference on Digital Government Research*, Virtual Event, Republic of Korea, 2022.

[32] J. Hickman, "A New Set of Android 10 Images and Files," [Online]. Available: https://digitalcorpora.org/corpora/cell-phones/android10/.

[33] https://github.com/Farhan7843/Privacy-Preserving-Digital-Forensics-A-FHE-Based-Fra
git