EFFICIENT AUDITING SCHEME FOR SECURE DATA STORAGE IN FOG-TO-CLOUD COMPUTING

1 L. Jagajeevan Rao, Associate Professor
2 Ch. Gunadeep 3 K. Pavan Kumar 4 G. Bala Krishna 5 B. Sindhu
Miracle Educational Group of Institutions, Vizianagaram, A.P, India

ABSTRACT

Fog-to-cloud computing has now become a new cutting-edge technique along with the rapid popularity of Internet of Things (IoT). Unlike traditional cloud computing, fog-to-cloud computing needs more entities to participate in, including mobile sinks and fog nodes except for cloud service provider (CSP). Hence, the integrity auditing in fog-to-cloud storage will also be different from that of traditional cloud storage. In the recent work of Tian et al., they took the first step to design public auditing system for fog-to-cloud computing. However, their scheme becomes very inefficient since they uses intricate public key cryptographic techniques, including bilinear mapping, proof of knowledge etc. In this paper, we design a general and more efficient auditing system based on MAC and HMAC, both of which are popular private key cryptographic techniques. By implementing MAC and HMAC, we give a concrete instantiation of our auditing system. Finally, the theoretical analysis and experiment results show that our proposed system has more efficiency in terms of communication and computational costs.

1. INTRODUCTION

Fog computing, which is first proposed by Bonomi et al. in 2012 [6], has now been a popular technique for kinds of industrial fields based on Internet-of Things (IoT) devices [15], [16], [19], [32]. As a middleware between IoT devices and clouds, fog computing nodes have their own basic computing, storage as well as resources to achieve the requirements for data preprocessing and transmission. Therefore, the model of fog-to-cloud computing emerges as an attractive solution for data storage in some resource-constrain large-scale industrial applications.

However, fog-to-cloud computing has also to face some classical problems appeared in traditional cloud computing. One of the most famous concerns is how to ensure the integrity of stored in cloud service provider (CSP). The reasons as follows. Some CSP may try to conceal the fact that some important data of IoT devices or fog nodes has been lost or corrupted due to kinds of internal or external attacks [25]. Hence, developing efficient auditing techniques for secure data storage in fog-to-cloud computing are also very necessary and significant just like in traditional cloud computing.

Although, in past years, many auditing schemes are presented for traditional cloud storage [12], [22], [25], [26], [31], [33], including many private and public auditing schemes, all of them are not directly applicable to fog-to-cloud computing for two main reasons [23], [24]. The first one is that the data from IoT is generated by various devices and hence it is inadvisable for those users (or data owners) to first retrieve these data and generate corresponding authenticators before outsourcing. The second one, which is also more important, is that the existing auditing systems do not involve fog computing nodes, which are rather crucial entities for fog-to-cloud computing because those nodes can help to efficiently process and rapidly transmit for large-scale of IoT data. Hence, it is urgent to develop new auditing techniques to ensure data's integrity for fog-to-cloud computing. In recent work of [23], Tian et al. took the first step to this direction and try to fill this gap. In
fact, they designed a privacy-preserving public auditing system based on bilinear mapping and the so-called tag-transforming strategy. In addition, they also evaluated the performances of their scheme by theoretical analysis and comprehensive experiments. It is well-known that, in public auditing scheme, the task to verify the integrity of users' data is suitable to be outsourced to another authorized third-party auditor (TPA), which may have more professional knowledge on auditing and more computational resources. However, it should also be noted that, generally speaking, public auditing systems have lower efficiencies than private ones. Just as Zhang et al. illustrated in [33], for a same data file, the time consumptions for proving, verifying and outsourcing in public auditing scheme are hundreds (or even thousands) of times of the corresponding process in their private scheme. Hence, in some pursuing-efficiency scenarios, especially for theresource-constrained mobile sinks in fog-to-cloud computing, we believe the private auditing system may be more popular. Therefore, it is also necessary and significant to design efficient private auditing schemes for the fog-to-cloud computing.

In this paper, we try to take the step to this direction. More specifically, we propose a new auditing system base on private authentication techniques: message authentication code (MAC) [14] and homomorphic MAC (HMAC) [2], [8], [10] schemes, both of which are important primitives in cryptography. The MAC technique is used in the transmission process between mobile sinks and fog nodes while the HMAC scheme is used to verify the integrity of data blocks stored in CSP. Since a common private key is needed for the parties in MAC or HMAC when generating or verifying the tags, this model is not suitable to introduce TPA into it.

Moreover, we give a concrete instantiation of the system by instantiating the hash-based MAC scheme in [14] and the efficient HMAC scheme designed by Agrawal and Boneh in [2].

Finally, we also analyze the performances of our proposed system and compare them with that of Tian et al. as well as two related traditional cloud auditing schemes in [20] and [18]. The experiment results show that our system outperformed Tian et al.'s system in terms of communication costs and computational efficiency. Moreover, our protocol is suitable for fog-to-cloud computing and hence prior to the two schemes in [18], [20].

2. LITERATURE SURVEY

One of the earliest work to consider the integrity of data stored in remote clouds is proof of retrievability (PoR) suggested by Jues and Kaliski [13]. In PoR, one can combine error-correcting code with spot-checking of data blocks to ensure the data's integrity. But this technique only supports a limited number of verification operations. At the same time, Ateniese et al. proposed provable data possession (PDP) based RSA-homomorphic authenticators, which can support both unlimited number of challenges and public auditing [3]. Subsequently, many works focused on the improvement of communication efficiency [4], [7], [11], [20].

Some other researches considered the dynamic update of PDP schemes [12], [22], [26], [28]. To support data dynamics, kinds of authenticated data structures are widely introduced into the public auditing schemes. For example, in 2011, Wang et al. presented the Merkle-hash-tree-based public auditing for dynamic data [26]. Later, Zhu et al. proposed a new data structure, called index hash table, to achieve data dynamics [34]. In 2017, Tian et al. further suggested a two-dimensional data structure, named dynamic hash table, to achieve both public auditing and dynamic data updating [22]. At the same year, Shen et al. proposed another novel structure, which includes a doubly linked info table and a location array, to achieve dynamic data [21]. However, few of them can be directly extended to achieve efficient and secure verification for data storage in the fog-to-cloud based IoT scenarios, although there are fruitful schemes suggested in the traditional cloud storage.
The two main reasons are as follows. First, in fog-to-cloud case, the data are usually generated by various IoT devices, instead of the data owners themselves. Second, some new entities, like fog nodes, are introduced and also play important roles for processing and transmission in fog-to-cloud scenario. But in the traditional cloud storage, they are never considered. Therefore, in the recent works, Tian et al., [23] and Kashif and Mohammed [18] respectively filled this gap in the public auditing setting based on different techniques. Nevertheless, the more efficient private key auditing schemes are not considered in both papers. As for the fog-computing, we note that, in the recent work [27], Wu et al. proposed a fog-computing-enabled cognitive network functions virtualization approach for an information-centric future Internet and also designed a communication scheme between the fog nodes and the future Internet Nodes for the forwarding process.

[1] J. A. Akinyele, C. Garman, I. Miers, M. W. Pagano, M. Rushanan, M. Green, and A. D. Rubin, “Charm: A framework for rapidly prototyping cryptosystems,” J. Cryptogr. Eng., vol. 3, no. 2, pp. 111–128, Jun. 2013.

We describe Charm, an extensible framework for rapidly prototyping cryptographic systems. Charm provides a number of features that explicitly support the development of new protocols, including support for modular composition of cryptographic building blocks, infrastructure for developing interactive protocols, and an extensive library of re-usable code. Our framework also provides a series of specialized tools that enable different cryptosystems to interoperate. We implemented over 40 cryptographic schemes using Charm, including some new ones that, to our knowledge, have never been built in practice. This paper describes our modular architecture, which includes a built-in benchmarking module to compare the performance of Charm primitives to existing C implementations. We show that in many cases our techniques result in an order of magnitude decrease in code size, while inducing an acceptable performance impact. Lastly, the Charm framework is freely available to the research community and to date, we have developed a large, active user base.

[2] S. Agrawal and D. Boneh, “Homomorphic MACs: MAC-based integrity for network coding,” in Applied Cryptography and Network Security, (Lecture Notes in Computer Science), vol. 5536. Berlin, Germany: Springer, 2009, pp. 292–305.

Network coding has been shown to improve the capacity and robustness in networks. However, since intermediate nodes modify packets en-route, integrity of data cannot be checked using traditional MACs and checksums. In addition, network coded systems are vulnerable to pollution attacks where a single malicious node can flood the network with bad packets and prevent the receiver from decoding the packets correctly. Signature schemes have been proposed to thwart such attacks, but they tend to be too slow for online per-packet integrity.

Here we propose a homomorphic MAC which allows checking the integrity of network coded data. Our homomorphic MAC is designed as a drop-in replacement for traditional MACs (such as HMAC) in systems using network coding.

[3] G. Ateniese, R. Burns, R. Curtmola, Joseph Herring, L. Kissner, Z. Peterson, and D. Song, “Provable data possession at untrusted stores,” in Proc. 14th ACM Conf. Comput. Commun. Secur., Alexandria, VA, USA, 2007, pp. 598–609.

We introduce a model for provable data possession (PDP) that allows a client that has stored data at an untrusted server to verify that the server possesses the original data without retrieving it. The model generates probabilistic proofs of possession by sampling random sets of blocks from the server, which drastically reduces I/O costs. The client maintains a constant amount of metadata to verify the proof. The challenge/response protocol transmits a small, constant amount of data, which minimizes network communication. Thus, the PDP model for remote data checking supports large data sets in widely-distributed storage system.

We present two provably-secure PDP schemes that are more efficient than previous solutions, even
when compared with schemes that achieve weaker guarantees. In particular, the overhead at the server is low (or even constant), as opposed to linear in the size of the data. Experiments using our implementation verify the practicality of PDP and reveal that the performance of PDP is bounded by disk I/O and not by cryptographic computation.

[4] G. Ateniese, S. Kamara, and J. Katz, “Proofs of storage from homomorphic identification protocols,” in Advances in Cryptology. Berlin, Germany: Springer, 2009, pp. 319–333.

Proofs of storage (PoS) are interactive protocols allowing a client to verify that a server faithfully stores a file. Previous work has shown that proofs of storage can be constructed from any homomorphic linear authenticator (HLA). The latter, roughly speaking, are signature/message authentication schemes where ‘tags’ on multiple messages can be homomorphically combined to yield a ‘tag’ on any linear combination of these messages.

We provide a framework for building public-key HLAs from any identification protocol satisfying certain homomorphic properties. We then show how to turn any public-key HLA into a publicly-verifiable PoS with communication complexity independent of the file length and supporting an unbounded number of verifications. We illustrate the use of our transformations by applying them to a variant of an identification protocol by Shoup, thus obtaining the first unbounded-use PoS based on factoring (in the random oracle model).

[5] A. F. Barsoum and M. A. Hasan, “Provable multicopy dynamic data possession in cloud computing systems,” IEEE Trans. Inf. Forensics Security, vol. 10, no. 3, pp. 485–497, Mar. 2015.

Increasingly more and more organizations are opting for outsourcing data to remote cloud service providers (CSPs). Customers can rent the CSPs storage infrastructure to store and retrieve almost unlimited amount of data by paying fees metered in gigabyte/month. For an increased level of scalability, availability, and durability, some customers may want their data to be replicated on multiple servers across multiple data centers. The more copies the CSP is asked to store, the more fees the customers are charged. Therefore, customers need to have a strong guarantee that the CSP is storing all data copies that are agreed upon in the service contract, and all these copies are consistent with the most recent modifications issued by the customers. In this paper, we propose a map-based provable multicopy dynamic data possession (MB-PMDDP) scheme that has the following features: 1) it provides an evidence to the customers that the CSP is not cheating by storing fewer copies; 2) it supports outsourcing of dynamic data, i.e., it supports block-level operations, such as block modification, insertion, deletion, and append; and 3) it allows authorized users to seamlessly access the file copies stored by the CSP. We give a comparative analysis of the proposed MB-PMDDP scheme with a reference model obtained by extending existing provable possession of dynamic single-copy schemes. The theoretical analysis is validated through experimental results on a commercial cloud platform. In addition, we show the security against colluding servers, and discuss how to identify corrupted copies by slightly modifying the proposed scheme.

[6] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, “Fog computing and its role in the Internet of Things,” in Proc. 1st Ed. MCC Workshop Mobile Cloud Comput., New York, NY, USA, 2012, pp. 13–16.

Fog Computing extends the Cloud Computing paradigm to the edge of the network, thus enabling a new breed of applications and services. Defining characteristics of the Fog are: a) Low latency and location awareness; b) Wide-spread geographical distribution; c) Mobility; d) Very large number of nodes, e) Predominant role of wireless access, f) Strong presence of streaming and real time applications, g) Heterogeneity. In this paper we argue that the above characteristics make the Fog the appropriate platform for a number of critical Internet of Things (IoT) services and applications, namely, Connected Vehicle, Smart Grid, Smart Cities, and, in general, Wireless Sensors and Actuators Networks (WSANs).

3. PROBLEM STATEMENT

Jues and Kaliski [13]. In PoR, one can combine error-correcting code with spot-
checking of data blocks to ensure the data’s integrity. But this technique only supports a limited number of verification operations. At the same time, Atniese et al. proposed provable data possession (PDP) based RSA-homomorphic authenticators, which can support both unlimited number of challenges and public auditing [3].

Subsequently, many works focused on the improvement of communication efficiency [4], [7], [11], [20]. Some other researches considered the dynamic update of PDP schemes [12], [22], [26], [28]. To support data dynamics, kinds of authenticated data structures are widely introduced into the public auditing schemes. For example, in 2011, Wang et al. presented the Merkle-hash-tree-based public auditing for dynamic data [26]. Later, Zhu et al. proposed a new data structure, called index hash table, to achieve data dynamics [34]. In 2017, Tian et al. further suggested a two-dimensional data structure, named dynamic hash table, to achieve both public auditing and dynamic data updating [22]. At the same year, Shen et al. proposed another novel structure, which includes a doubly linked info table and a location array, to achieve dynamic data [21].

However, few of them can be directly extended to achieve efficient and secure verification for data storage in the fog-to-cloud based IoT scenarios, although there are fruitful schemes suggested in the traditional cloud storage. The two main reasons are as follows. First, in fog-to-cloud case, the data are usually generated by various IoT devices, instead of the data owners themselves. Second, some new entities, like fog nodes, are introduced and also play important roles for processing and transmission in fog-to-cloud scenario. But in the traditional cloud storage, they are never considered.

Therefore, in the recent works, Tian et al., [23] and Kashif and Mohammed [18] respectively filled this gap in the public auditing setting based on different techniques. Nevertheless, the more efficient private key auditing schemes are not considered in both papers.

3.1 Limitation of system

The system was not implemented Attribute Based Encryption and data auditing techniques on outsourced data. The system is less security due to lack of Identity-Based Encryption.

4. PROPOSEDSYSTEM

In the proposed system, the system tries to take the step to this direction. More specifically, we propose a new auditing system based on private authentication techniques: message authentication code (MAC) [14] and homomorphic MAC (HMAC) [2], [8], [10] schemes, both of which are important primitives in cryptography. The MAC technique is used in the transmission process between mobile sinks and fog nodes while the HMAC scheme is used to verify the integrity of data blocks stored in CSP. Since a common private key is needed for the parties in MAC or HMAC when generating or verifying the tags, this model is not suitable to introduce TPA into it. Moreover, we give a concrete instantiation of the system by instantiating the hash-based MAC scheme in [14] and the efficient HMAC scheme designed by Agrawal and Boneh in [2].

4.1 Advantages

DATA PREVENTION. DYNAMIC UPDATE AND PREVENTING REPLAY ATTACKS. An Efficient Data Auditing and Recovery techniques to provide more security on the remote data sender data.

5. SYSTEM ARCHITECTUR
6. IMPLEMENTATION

6.1 SENDER (OWNER)

In this module sender will have to register and get authorized before he performs any operations. After the authorization the sender can upload file with trapdoor and will have the update, delete, verify and recovery options for the file uploaded.

6.2 CSP

In this module CSP will issue permission for both owner (Sender) and user (Receiver). And view the file uploaded and the attackers related to files in cloud. View the files in decrypted format and with the corresponding secret keys and its transactions.

6.3 RECEIVER (USER)

In this module, User has to register and login, and search for the files by entering keyword and request secret key and download the particular file from the cloud if both secret key and the decryption permissions are provided.

6.4 FOG

Views all the files decrypt permission request form the users and provide permission and view its related metadata and the transactions related to the requests from users.

6.5 KGC

In this module the private key generator generates the secret key. It splits the key into two parts such as pkey1 and pkey2. This generated key is unique for different users for same file and view all the generated secret keys and the transactions related to it.

7. ALGORITHMS USED

7.1. HOMOMORPHIC MAC

Informally, a homomorphic MAC scheme is an authentication technology, which allows ‘‘legal’’ users to verify the correctness of the generated tag t for a message v, which in fact is an (n + s)-dimensional vector in some finite field Fq, and recompute a new tag on a combined message. Formally, a (q, n,s) homomorphic MAC scheme consists of four PPT algorithms HMAC-KeyGen, HMAC, HCombine and HVerify, which have the following forms.

- HMAC-KeyGen : For the input λ, this algorithm generates and outputs a secret key K.

- HMAC : Take as inputs of a secret key K, an identifier id, an augmented vector v ∈ F n+s q , and j ∈ [s] indicating that v is the the j-th basis vector of the vector space identified by id. This algorithm will output a tag T for v.

- HCombine : For the inputs of \( \gamma \) (\( \gamma < s \)) constants \( r_1, \ldots, r_\gamma \in F_q \), vectors \( v_1, \ldots, v_\gamma \in F_{n+s} q \) and the corresponding tags \( T_1, \ldots, T_\gamma \), this algorithm outputs a tag T for the combined vector \( y := \sum \gamma_{i=1} r_i v_i \in F_{n+s} q \).

- HVerify : For the inputs of a secret key K, an identifier id, a vector \( y \in F_{n+m} q \) and a tag T , this algorithm outputs 0 (reject) or 1 (accept). The correctness requires that, for any secret key K, \( r_1, \ldots, r_\gamma \in F_q \), it holds that \( 1 \leftarrow HVerify \)

8. OUTPUT RESULTS
9. CONCLUSION

In this paper, we propose an efficient auditing system for fog-to-cloud computing. Although our system is not public auditing, it obviously outperforms the one proposed by Tian et al. in terms of communication and computational efficiencies. The simulation results illustrate the computational efficiency. We believe that our proposed system must be an interesting choice for securely storage of data in fog-to-cloud computing.

10. REFERENCES

[1] V. Subrahmanian and S. Kumar, "Predicting human behavior: The next frontiers," *Science*, vol. 355, no. 6324, p. 489, 2017.

[2] H. Lauw, J. C. Shafer, R. Agrawal, and A. Ntoulas, "Homophily in the digital world: A LiveJournal case study," *IEEE Internet Comput.*, vol. 14, no. 2, pp. 15-23, Mar./Apr. 2010.

[3] M. A. Al-Garadi, K. D. Varathan, and S. D. Ravana, "Cybercrime detection n online communications: The experimental case of cyberbullying detection in the Twitter network," *Comput. Hum. Behav.*, vol. 63, pp. 433-443, Oct. 2016.

[4] L. Phillips, C. Dowling, K. Shaffer, N. Hodas, and S. Volkova, "Using social media to predict the future: A systematic literature
review," 2017, arXiv:1706.06134. [Online]. Available: https://arxiv.org/abs/1706.06134

[5] H. Quan, J. Wu, and Y. Shi, "Online social networks & social network services: A technical survey," in Pervasive Communication Handbook. Boca Raton, FL, USA: CRC Press, 2011, p. 4.

[6] J. K. Peterson and J. Densley, "Is social media a gang? Toward a selection, facilitation, or enhancement explanation of cyber violence," Aggression Violent Behav., 2016.

[7] BBC. (2012). Huge Rise in Social Media. [Online]. Available: http://www.bbc.com/news/uk-20851797

[8] P. A. Watters and N. Phair, "Detecting illicit drugs on social media using automated social media intelligence analysis (ASMIA)," in Cyberspace Safety and Security. Berlin, Germany: Springer, 2012, pp. 66_76.

[9] M. Fire, R. Goldschmidt, and Y. Elovici, "Online social networks: Threats and solutions," IEEE Commun. Surveys Tuts., vol. 16, no. 4, pp. 2019_2036, 4th Quart., 2014.

[10] N. M. Shekokar and K. B. Kansara, "Security against sybil attack in social network," in Proc. Int. Conf. Inf. Commun. Embedded Syst. (ICICES), 2016, pp. 1_5.

[11] J. Ratkiewicz, M. Conover, M. Meiss, B. Gonçalves, A. Flammini, and F. Menczer, "Detecting and tracking political abuse in social media," in Proc. 5th Int. AAAI Conf. Weblogs Social Media, 2011, pp. 297_304.

[12] A. Aggarwal, A. Rajadesingan, and P. Kumarakugur, "PhishAri: Automatic realtime phishing detection on Twitter," in Proc. eCrime Res. Summit (eCrime), Oct. 2012, pp. 1_12.

[13] S. Yardiet et al., "Detecting spam in a Twitter network," First Monday, Jan. 2009. [Online]. Available: https://rstmonday.org/article/view/2793/2431

[14] C. Yang, R. Harkreader, J. Zhang, S. Shin, and G. Gu, "Analyzing spammers' social networks for fun and pro_t: A case study of cyber criminal ecosystem on twitter," in Proc. 21st Int. Conf. World Wide Web, 2012, pp. 71_80.

[15] G. R. S. Weir, F. Toolan, and D. Smedd, "The threats of social networking: Old wine in new bottles?" Inf. Secur. Tech. Rep., vol. 16, no. 2, pp. 38_43, 2011.

[16] M. J. Magro, "A review of social media use in e-government," Administ. Sci., vol. 2, no. 2, pp. 148_161, 2012.

[17] M. Dadvar, D. Trieschnigg, R. Ordelman, and F. de Jong, "Improving cyberbullying detection with user context," in Advances in Information Retrieval. Berlin, Germany: Springer, 2013, pp. 693_696.

[18] Y. Chen, Y. Zhou, S. Zhu, and H. Xu, "Detecting offensive language in social media to protect adolescent online safety," in Proc. Int. Conf Privacy, Secur., Risk Trust (PASSAT), Sep. 2012, pp. 71_80.

[19] V. S. Chavan and S. S. Shylaja, "Machine learning approach for detection of cyber-aggressive comments by peers on social media network," in Proc. Int. Conf. Adv. Comput., Commun. Inform. (ICACCI), Aug. 2015, pp. 2354_2358.

[20] W. Dong, S. S. Liao, Y. Xu, and X. Feng, "Leading effect of social media for nancial fraud disclosure: A text mining based analytics," in Proc. AMCIS, San Diego, CA, USA, 2016.

[21] M. S. Rahman, T.-K. Huang, H. V. Madhyastha, and M. Faloutsos, "FRAppE: Detecting malicious Facebook applications," in Proc. 8th Int. Conf. Emerg. Netw. Exp. Technol., 2012, pp. 313_324.

[22] S. Abu-Nimeh, T. Chen, and O. Alzubi, "Malicious and spam posts in online social networks," Computer, vol. 44, no. 9, pp. 23_28, Sep. 2011.

[23] B. Doerr, M. Fouz, and T. Friedrich, "Why rumors spread so quickly in social networks," Commun. ACM, vol. 55, no. 6, pp. 70_75, Jun. 2012.
[24] J. W. Patchin and S. Hinduja, *Words Wound: Delete Cyberbullying and Make Kindness Go Viral*. Golden Valley, MN, USA: Free Spirit Publishing, 2013.

[25] J. Cheng, C. Danescu-Niculescu-Mizil, and J. Leskovec, “Antisocial behavior in online discussion communities," in *Proc. 9th Int. AAAI Conf. Web Social Media*, Apr. 2015.

[26] S. Liu, J. Zhang, and Y. Xiang, “Statistical detection of online drifting Twitter spam: Invited paper," in *Proc. 11th ACM Asia Conf. ComputCommun. Secur.*, 2016, pp. 1_10.

[27] Z. Miller, B. Dickinson, W. Deitrick, W. Hu, and A. H. Wang, “Twitter spammer detection using data stream clustering," *Inf. Sci.*, vol. 260, p. 64_73, Mar. 2014.

[28] M. Jiang, S. Kumar, V. S. Subrahmanian, and C. Faloutsos, “KDD 2017 tutorial: Data-driven approaches towards malicious behavior modeling," *Dimensions*, vol. 19, p. 42, 2017.

[29] S. Y. Jeong, Y. S. Koh, and G. Dobbie, “Phishing detection on Twitter streams," in *Proc. Paci_c_Asia Conf. Knowl. Discovery Data Mining*. Cham, Switzerland: Springer, 2016, pp. 141_153.

[30] I. Frommholz, H. M. Al-Khateeb, M. Potthast, Z. Ghasem, M. Shukla, and E. Short, “On textual analysis and machine learning for cyberstalking detection," *Datenbank-Spektrum*, vol. 16, no. 2, pp. 127_135, 2016.