SOCIETY FOR SCIENCE AND EDUCATION
UNITED KINGDOM

TNC TRANSACTIONS ON NETWORKS AND COMMUNICATIONS

VOLUME 8, NO. 4
ISSN: 2054 -7420

Tracking of Malicious Attacks on Data Online: A Systematic Review

Isah Abdulkadir Onivehu, Alhassan John Kolo, Idris Ismaila, Adebayo Olawale Surajudeen
Department of Cyber Security Science, School of Information and Communication Technology, Federal University of Technology, Minna, Nigeria;
ao.isah@futminna.edu.ng; jkalhassan@futminna.edu.ng; ismi.idris@futminna.edu.ng; waleadebayo@futminna.edu.ng

ABSTRACT

Tracking of computer network system attacks is a proactive measure to protect against attacks on data, that are basically encrypted for confidential security reasons, while in transit on the computer information channel. Cyber security threat continues to increase in direct proportion to the rate at which internet based services are deployed. In this systematic review, 53 research papers from reputable publishers were downloaded out of which 41 papers that are closely related to tracking of malicious attackers on encrypted data online were review under the consideration of attacks on encrypted data, and tracking malicious attacks; with respect to proposed technique, problem addressed, comparison to existing methodology, parameters used, major findings and then limitations and future knowledge. The authors then deduce the classification of four varying types of attacks (Keyword Guessing Attack, Selective opening attacks, Leakage-Abuse Attacks, and Key Reinstallation Attacks) from the review, to narrow down research into the future countermeasures for these attacks. 11 research papers actual discuss countermeasures for these classification types, with Keyword Guessing Attack being the focus of 6 research work, Selective Opening Attacks have 3 papers trying to solve vulnerabilities permitting such attacks, 2 papers aimed research solutions at Leakage-Abuse Attacks, and Key Reinstallation Attacks, has mention but none of the papers reviewed proffer mitigation techniques. The remaining 30 papers concentrated discussions on general attacks on encrypted data. Inclining future research attention to the four kinds of attacks against encrypted data will improve attack detection contrary to the commonly post-mortem approach.

Keywords: Encryption, Network, Vulnerabilities, Attack, Countermeasures, Security.

1 Introduction

Many web users routinely transmit and store sensitive data online, such as bank accounts, health records and private correspondence [1]. Servers that store such data are a tempting target for cybercriminals: a single attack can yield valuable data, such as credit card numbers of users in millions [1]. The advent of network forensics envisioned several investigation methods for network security breaches and vulnerabilities [2]. Now-a-days government, academics and private organizations are investing a huge amount of money, lots of time and memory of computer system for information security [3]. The evolution

DOI: 10.14738/tnc.84.9463
Publication Date: 17th September 2020
URL: http://dx.doi.org/10.14738/tnc.84.9463

and sophistication of cyber-attacks need resilient and evolving cyber security schemes [4]. The confidentiality of the information stored in computer systems and sent through information channels is a matter of primary concern [5].

Real-time encryption encrypts or decrypts the data right before the data are sent or loaded without any user intervention [6]. To guarantee confidentiality, the generator (transmitter) must encrypt the information and the user end (receiver) must decrypt it. This process of encryption and decryption is carried out with symmetric algorithms, like DES (Data Encryption Standard), 3DES (Triple DES), Blowfish, Twofish, RC4 (developed by Ronald Rivest of RSA, is a shared key stream cipher algorithm requiring a secure exchange of a shared key), RC6 (a symmetric key block cipher derived from RC5, to meet the requirements of the AES competition), CAST (is a symmetric-key block cipher used in a number of products), Advanced Encryption Standard (AES) [5]. Advanced encryption standard (AES) is a widely used encryption algorithm [6].

Cyber-attacks [7] are becoming more attractive and can lead to large-scale (or global) systemic failures, resulting in loss of human life and social unrest as our dependence on information technology increases [7]. The ubiquity of networks has made us vulnerable to various network risks. For instance, rumours spread incredibly fast in online social networks, such as Facebook, Twitter and WhatsApp [8]. Computer viruses propagate throughout the Internet and infect massive network of computers [8]. In smart grids, isolated failures could lead to rolling blackouts in the networks [8]. Every year, tremendous damages caused by those risks have incurred tremendous losses to society in finance and labour [8].

As cyberspace based technologies are being utilized by different individuals, there is a propensity that they would be exposed to increasing security dangers. Since network systems are utilized by various individuals, there are expanding number of security issues and security of data on transition [9] which required the improvement of various intrusion detection frameworks.

2 Literature Review

2.1 Attacks on Encrypted Data

Huang and Li [10] proposed the idea of securing against insider keyword guessing attack using authenticated public key encryption scheme with keyword searches. The authentication is an improvement on the loopholes in the research work of [11] that could not protect against insider attack that seeks to recover the keywords through a trapdoor in an offline exhaustive guessing. The research work was not concerned about the real time tracking of the insider since it is more of an offline attacks.

Vanhoef and Piessens [12] introduced key reinstallation attack, an attack that abuses design or implementation flaws in cryptographic protocols to reinstall a key that is already in use. Several types of cryptographic Wi-Fi handshakes are affected by the attack. The authors prove that the traditional four-way handshakes are vulnerable to reinstallation attacks. The impact of nonce (one time passwords) reuse for the data confidentiality protocols of 802.11, present example of attack scenarios, discuss implementation specific vulnerabilities, explain why security proofs missed attacks used in the research work, and present countermeasures. These countermeasures are that the entity implementing the data-confidentiality protocol should check whether an already-in-use key is being installed. If so, it should not reset associated nonce (one time passwords) and replay counters. The second measure is to assure that

a particular key is only installed once into the entity implementing the data-confidentiality protocol during a handshake execution. However, a real time approach of flagging off key reinstallation attempt and then preventing the execution of the session can also mitigate the malicious attack.

Huang [13] argues that the concerns about privacy protection and data security are the primary restraining factors in the quest to subscribe to cloud computing. The authors identified selective opening attacks security as a phenomenon in cloud computing in which multiple senders encrypt individual or personal data with the public key of a single receiver, given the ciphertexts, the adversary is allowed to corrupt some of the senders, seeing not only their plaintexts but also the random keys used during the encryption. The security requirement of selective opening attacks (SOA) is that the privacy of the unopened data is preserved. On the other hand, the scenario of selective opening attacks is a challenge against non-malleability, a very important security notion for data security in cloud computing and public-key cryptography. The security requirement of non-malleability is that given a challenge ciphertext, it should be infeasible to generate a ciphertext vector whose decryption is meaningfully related to the corresponding challenge plaintext. The researchers were able to show that the secure PKE scheme proposed by [14] actually achieves security, and formalize the security notion of non-malleability under selective opening attacks (NM-SO security), and explore the relations between NM-SO security and the standard SOA security, the relations between NM-SO security and the standard non- malleability, and the relations among NM-SO security notions. Models for improving cloud computing security in relation to attacks against encrypted data through selective opening attacks were not achieved in the research work.

Grubbs [15] explains that due to the rising interests in outsourcing data to the cloud and the corresponding cases of attacks and data security breaches, information technology firms are keen to encrypting sensitive information to safe-keep it in databases or uploading to cloud services operated by third parties. Standard encryption mechanisms would, however, reduce the value of these databases and services by preventing them from doing useful database operations on the data. Order-preserving encryption (OPE) and its generalization order-revealing encryption (OPE/ORE) allow sorting, performing range queries, and filtering ciphertext data. The disadvantage of OPE and ORE is that such ciphertexts necessarily leak information about plaintexts. A seeming solution is to use so-called property-revealing encryption (PRE) schemes that allow limited operations over ciphertexts by making public specific properties of plaintexts. The research is able to launch leakage-abuse attacks in which frequently occurring plaintexts were recovered from OPE/ORE-encrypted databases most of the time. The setback in the work is little mention is made about countermeasures.

Grubbs [16] developed systematic method for the analysis of client-server applications that seeks to keep the confidentiality of sensitive user data from untrusted servers. This approach is applied to a framework that uses multi-key searchable encryption (MKSE) to engineer web applications on top of encrypted data. The authors demonstrated that the Popa-Zeldovich model for MKSE does not imply security against either passive or active attacks, Mylar-based Web applications reveal users' data and queries to passive and active adversarial servers, and Mylar is generically insecure against active attacks due to system design flaws. The paper does not proffer improved security solutions to the vulnerabilities discovered to which real time detection of attacks could serve as deterrence to potential hackers.

The explanation in [17] is that various protocols have been modelled to securely outsource database storage to a third party server, ranging from systems whose confidential security is based on strong cryptographic primitives such as fully homomorphic encryption or oblivious RAM, to more practical

implementations founded on searchable symmetric encryption, deterministic and order-preserving encryption. The authors deem it necessary to identify a formal understanding of the inherent efficiency and privacy trade off in outsourced database systems, independent of the details of the system. The researchers move further to propose abstract models that capture secure outsourced storage systems that reveals two basic sources of leakage, namely; access pattern and communication volume. However, countermeasures to these generic attacks were not discussed.

Pouliot and Wright [18] presents that to add end-to-end encryption to legacy applications without losing the convenience of full-text search, ShadowCrypt and Mimesis Aegis use cryptographic technique called efficiently deployable efficiently searchable encryption (EDESE) to provide standard full-text search system, to perform searches on encrypted data. EDESE schemes leak a great deal of statistical information about the encrypted messages and the keywords they contain. The authors show that requirement of matching plaintext keywords to the opaque cryptographic identifiers by the adversary as used in EDESE can be reduced to combinatorial optimization problem of weighted graph matching (WGM). The experimentation uses real email and chat data, to show how on the shelf WGM solvers can be used to accurately and recover hundreds of common plaintext keywords from a set of EDESE encrypted messages. Table 1 present the analysis of related materials on attacks against encrypted data.

Table 1. Analysis of related materials on attacks against encrypted data

S/N	Author(s) / References	Proposed technique	Problem addressed	Comparison methods	Major findings	Parameter used	Limitation
1	Huang, Q., & Li, H. (2017).	Public-key Authenticated Encryption with Keyword Search (PAEKS)	Inside Keyword Guessing Attacks	Boneh *et al.*'s public key encryption with keyword search (PEKS) scheme	The ability to authenticate encrypted data	Not specified	PAEKS schemes is not based on standard and well-accepted assumptions
2	Boneh, D., Boyen, X., & Shacham, H. (2004).	Public key encryption with keyword search (PEKS).	Inside Keyword Guessing Attacks	Not stated	The notion of public key encryption with keyword search	Not specified	An inside adversary may recover the keyword from a given trapdoor by exhaustively guessing the keywords offline
3	Vanhoef, M., & Piessens, F. (2017).	key reinstallation attack (KRA)	Vulnerability test	Not stated	Wi-Fi device is vulnerable to some variant of our attacks	Wi-Fi handshakes, Android 6.0	Determining the vulnerabilities of other protocol implementations to KRA. Counter-measures
4	Huang, *et al.*, (2017)	Non-malleability under	Vulnerability test	Fehr *et al.*, (2010) actually achieves	Show that the decryptio	NM-SOA security and	Real time tracking of SO attacks.

		selective opening attacks (NM-SOA security)		SIM-NM-SO-CCA2 security	n algorithm of the Fehr et al., scheme is invertible, though.	the standard SOA security	
5	Grubbs, P., Sekniqi, K., Bindschaedler, V., Naveed, M., & Ristenpart, T. (2017)	Leakage abuse attacks	Vulnerability test	Kerschbaum scheme	Attacks recover frequently occurring plaintexts most of the time.	Not highlighted	Formal analysis of inference attacks. Developing an adaptive inference attacks.
6	Grubbs, P., McPherson, R., Naveed, M., Ristenpart, T., & Shmatikov, V. (2016	Analyzing client-server applications hiding sensitive user data from untrusted servers.	Securing client-server applications	Mylar, a framework that uses multi-key searchable encryption (MKSE)	The Popa-Zeldovich model for MKSE does not secure against attacks.	Not stated	Real time tracking of attacks against web applications on top of encrypted data.
7	Kellaris, G., Kollios, G., Nissim, K., & O'neill, A. (2016).	Abstract models that capture secure outsourced storage systems	Vulnerability test	Not stated	Outsourced database systems are vulnerable to generic leakage attacks.	Not stated	Countermeasures were not suggested.
8	Pouliot, D., & Wright, C. V. (2016)	Combinatorial optimization problem of weighted graph matching (WGM)	Adversary's task of matching plaintext keywords to cryptographic identifiers used in EDESE can be reduced	Efficiently deployable efficiently searchable encryption (EDESE)	WGM solvers can be used to recover commonly used plaintext keywords.	ShadowCrypt, Mimesis Aegis, and of the-shelf WGM solvers.	Real time tracking of inference attacks.

2.2 Tracking Malicious Attacks

The research in [19] agrees that the need to locate the sources of distributed attack require an inefficient amount of time, and most often than not attackers are identified after a successful compromise of the computer network. The authors proposed a model for tracking back, to identify attackers and locating their distributed sources in real time. In the model, attacks and attackers are identified by monitoring

violations of malicious end users on the network bandwidth shares, predefined in the service level agreement. It enables network administrators to investigate malicious users that are actively connected and then to locate the host machines used as distributed sources of attack traffic. The research further developed a Mathematical model with which to evaluate the results of simulations. The time required to identify malicious users and locating host machines used as the actual sources of attack packets is found to be drastically reduced, using the model.

Scaife [20] present CryptoDrop as a quick response system for detecting and alerting users against suspicious file activities that can lead to ransom-ware attacks. The authors implemented the system by training the traffic flow to classify normal behavioural indicators. CryptoDrop can halt a process that appears to be tampering with large amount of user's data. Furthermore, the system is parameterized by combining a set of indicators commonly identified with ransom-ware, for proactive detection with low false positives. The analysis of papers that researched into the tracking of malicious attacks on encrypted data is shown in table 2.

Table 2. Tracking malicious attacks

S/N	Author(s) / References	Proposed technique	Problem addressed	Comparison methods	Major findings	Parameter used	Limitation
1	Ahmed, A. A., Sadiq, A. S., & Zolkipli, M. F. (2016).	Trackback model	Identifying attackers and locating their distributed sources in real time	Not stated	Reduced the required time for identifying malicious users and locating host machines	Bandwidth and time	The end-user domain for identifying and reporting connections of active attackers is an unsecure process.
2	Scaife, N., Carter, H., Traynor, P., & Butler, K. R. (2016)	CryptoDrop	Stopping Ransomware Attacks on User Data	Not stated	Careful analysis of ransomware behaviour can produce an effective detection system to mitigate the attacks	Real-world ransomware samples	Tracing the source of ransomeware attacks were not discussed.

3 Systematic Review Methodology

3.1 Metadata information in the Web Pages and Expansion of the Query

The systematic review methodology applied in this research work is that used in [21] for the comprehensive outlay, presentation and structuring of related research materials. This was made possible with the review methodology split into research questions, research strategy, and selection criteria. This research work is interested in answering the various types of attacks against encrypted data, the mitigation measures against these attacks, methods with which the countermeasures can be improved.

3.2 Research Strategy

This systematic literature review employed as a strategy, the need to distinguish reputable academic and research databases from predator resource materials, for the purpose of credibility and validity of research results and findings. The academic databases include related books, conference papers and journals.

3.3 Source of Research Data

In this systematic review, related papers are the research data and the source is academic research databases that include Google Scholar, Springer, ACM Digital Library, Taylor and Francis (T&F), Science direct, Elsevier, Research Gate, Scopus, IEEE Xplore, Wiley Online Library (WOL) and Citeseerx. An illustration of access to these research databases is shown in figure 1.

3.4 Selection and Sorting Criteria

Furthermore, a total of 286 papers were searched from all the research publishing databases mentioned earlier, and the numbers of papers downloaded were 53. All the papers cited and or reviewed were recorded against each of the database it is sourced from, totalling 41. The papers sorted out with respect to duplicated versions and downloads are 233; that is same papers retrieved from different databases. In answering the question of how relevant the topics are to the interest of this systematic review on real time tracking of malicious attacks on encrypted data online, and finally the congruence of the abstract to the aims and objectives of these review, 12 papers were reduced from the number downloaded, leaving the systematic survey with 41 papers for the research work.

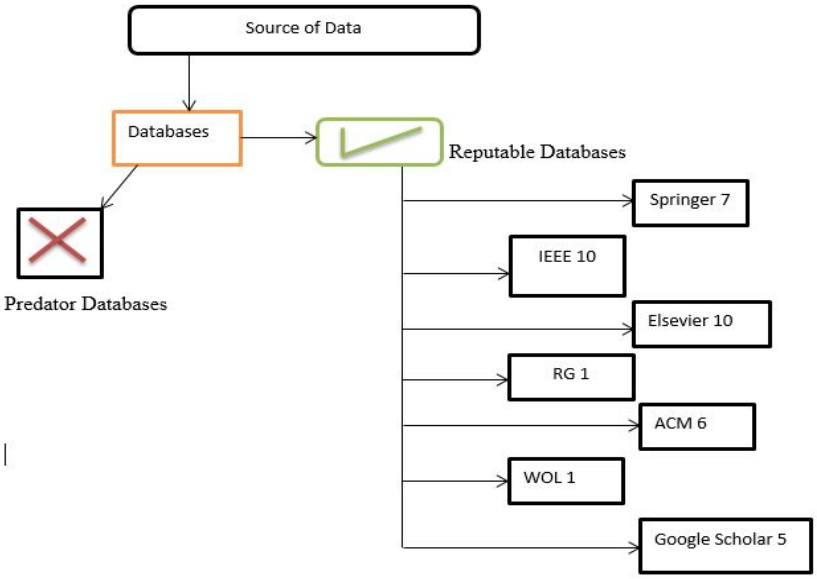

Figure 1: Academic Databases used for sourcing research papers

4 Classification of Attacks Against Encrypted Data

4.1 Keyword Guessing Attack

Pakniat [22] explains Public encryption keyword search (PEKS) methods are susceptible to attacks known as keyword guessing, in which a malicious intruder generates encrypted tags that corresponds to likely keywords. Then, by accessing a trapdoor, a match can be discovered and the searched keyword and files

containing it can be determined. Keywords belong to the set of words whose search space is small and thus a potentially successful attack is feasible [22]. The author in this survey, reviewed the concept of searchable encryption, the description of keyword guessing attack and the vulnerability of PEKS schemes to such attacks are discussed, highlighting drawback, and future research directions.

[23] improves the security of encrypted data using keyword search in designated servers by introducing the use of a scheme in nonce is attached to the keyword search to fend off malicious keyword guessing. While [24] proposed an expressive searchable public-key encryption scheme in groups that are in prime order that enables the formulation of policies guarding safe keyword search. The authors used Charm [25], a quick prototyping tool as methodology to implement the proposed scheme.

[8] proposed searchable encrypted keywords against insider attacks (SEK-IA) by rebuilding the security model of SEK-IA and a concrete constant size trapdoor as a feature. [26] worked on the existing PEKS scheme that is vulnerable to insider KGA. The authors proposed new technique to plug the loopholes that allows insider KGA in PEKS, using well defined algorithms.

[27] suggested cost-efficient secured channel free searchable encryption (SCF-PEKS) scheme for the sharing of electronic medical records. Although, there is the existence of SCF-PEKS solutions, this paper effect the reduction of storage overhead and improved computational performance to facilitate against keyword guessing attack in electronic medical records.

The security of searchable public key encryption scheme without certificate, for internet of things (IoT) environments by [28] is examined by [29] to discover that the scheme is not secured against an off-line keyword guessing attack. [29] then proposed an improvement. Table 3 present the analysis of research work against keyword guessing attacks.

Table 3. Analysis of research work against keyword guessing attacks

S/N	Author(s) / References	Proposed technique	Problem addressed	Comparison methods	Major findings	Parameter used	Limitation
1	Pakniat, N. (2016).	Survey	Attempts made to overcome vulnerability of PEKS schemes to such attacks are discussed.	Not stated	Finally, open problems and future work directions.	Not stated	No countermeasures offered.
2	Andola, N., Prakash, S., Venkatesan, S., & Verma, S. (2017	Nonce based keyword search scheme	Keyword guessing attacks	Trapdoor in-distinguish-ability (TD-IND).	Removing the weakness of ON-KGA, enhancing the security model for TD-IND.	Not stated	It favours a post-mortem approach to security and not real-time.

3	Jiang, P., Mu, Y., Guo, F., & Wen, Q. Y. (2017).	Searchable encrypted keywords against insider attacks (SEK-IA) framework	Insider attacks against searchable encrypted keywords	Public key encryption with keyword search (PEKS) schemes	Server cannot launch insider attacks to distinguish the keyword from a trapdoor.	Not stated	It favours a post-mortem approach to security and not real-time.
4	Sun, L., Xu, C., Zhang, M., Chen, K., & Li, H. (2018).	In-distinguishability obfuscation	Insider keyword guessing attacks	Not specified	Resisting insider KGA in PEKS.	Not stated	It follows the traditional detection of attacks after the damage is done
5	Wu, Y., Lu, X., Su, J., & Chen, P. (2016).	Secure channel free searchable encryption (SCF-PEKS) scheme	Keyword guessing attack,	Not specified	Preserving the privacy of electronic medical records (EMRs)	Memory space and time of execution	It follows the traditional detection of attacks after the damage is done
6	Wu, T. Y., Chen, C. M., Wang, K. H., & Wu, J. M. T. (2019).	Certificateless searchable public key encryption scheme	Keyword guessing attack.	Ma, M., He, D., Khan, M. K., & Chen, J. (2018).	Proposed an enhancement based on the Ma *et al.*, scheme	Not highlighted	Real time detection of keyword guessing activities

4.2 Leakage-Abuse Attacks

Rompay [30] reviewed Multi-User Searchable Encryption (MUSE) situation in which many users upload and search data in a cloud-based environment, many existing solutions have a common leakage and access pattern leakage. The authors also prove this vulnerability against existing software.

Bost and Fouque [31] addresses the problem of leakage abuse attacks by proposing an analysis of existing leakage abuse attacks and proffer methods with which to thwart, detect and counter in novel security definitions. Then, provide provable security of some schemes with specific leakage profile against some common classes of leakage abuse attacks.

Giraud [32] reviewed the leakage hierarchy introduced by [33], and thereafter launch penetration attacks on the symmetric keyword searchable encryption schemes of L4, L3 and L2 leakage profiles which are deployed in commercial cloud solutions. The penetration testing reveals devastating effects on real world data sets even with passive attacks with small knowledge of plaintexts sample. Table 4 present the analysis of research work against keyword guessing attacks.

Table 4. Analysis of leakage abuse research work

S/N	Author(s) / References	Proposed technique	Problem addressed	Comparison methods	Major findings	Parameter used	Limitation
1	Van Rompay, C., Molva, R., & Önen, M. (2017).	Penetration testing of Multi-User Searchable Encryption (MUSE)	Leakage abuse attack detection	Not specified	Most schemes reveal more than the access pattern, and can thus be exposed to powerful attacks.	Not stated	The work was not compared against any specific existing scheme for performance evaluation
2	Bost, R., & Fouque, P. A. (2017).	Analysis of existing leakage abuse attacks	Thwarting leakage abuse attacks	Not stated	Counter-measures can be implemented efficiently, and easily applied to existing searchable encryption schemes.	Not stated	The work was not compared against any specific existing scheme for performance evaluation
3	Giraud, M., Anzala-Yamajako, A., Bernard, O., & Lafourcade, P. (2017).	Passive attacks of L4, L3 and L2 schemes used in CipherCloud	Vulnerability test	(Zhang *et al.*, 2016) (Cash *et al.*, 2015; Islam *et al.*, 2012; Pouliot and Wright, 2016)	Analysis of existing attacks to highlight the gap of security that exists.	Not highlighted	The work was not compared against any specific existing scheme for performance evaluation.

4.3 Selective Opening Attacks

[34] study simulation-based selective opening security for receivers of public key encryption (PKE) schemes under chosen-ciphertext attacks (SIM-SO-CCA), thereby showing that some known PKE schemes meet SIM-SO-CCA security. Then, the notion of master-key SOA security for identity-based encryption (IBE) was introduced. [35] determines the fact that all chosen plaintext attack secure schemes are not all secure against selective opening attacks. The researchers' contrived scheme relies on strong assumptions of public-coin differing inputs obfuscation and a certain type of correlation intractable hash functions. Table 5 The Analysis of selective opening attacks research work.

Table 5. Analysis of selective opening attacks research work

S/N	Author(s) / References	Proposed technique	Problem addressed	Comparison methods	Major findings	Parameter used	Limitation
1	Huang, Z., Lai, J., Chen, W., Au, M. H., Peng, Z., & Li, J. (2018).	Master-key selective opening attack (SOA) security	Selective opening attacks	Simulation-based selective opening security	Identity-based encryption (IBE)	Not stated	Real time detection of SOA
2	Hofheinz, D., Rao, V., & Wichs, D. (2016).	Contrived encryption Hofheinz & Rupp (2014) scheme, which gives a chosen ciphertext attack (CCA) secure scheme that is not indistinguishable selective opening CCA secure.	Selective opening attacks	EUROCRYPT '12)	Chosen plaintext attack (CPA) secure but it is not in-distinguishability – selective opening attack secure (IND-SOA) secure.		counterexample for SOA-K security without relying on a scheme with common public parameters.

4.4 Discussion of Results

Comparing the numbers of papers that shows interest in the four classification of attacks, namely; Keyword guessing attack (KGA), Leakage-Abuse Attacks (LAA), Selective opening attacks (SOA), key reinstallation attacks (KRA) as highlighted in this research, Table 6 presents the numbers of papers available for reviewed against each of the attack. Also, figure 2 is the graphical representation of papers and the type of attack discussed table 6.

Table 6: Papers and the type of attacks discussed.

S/N	Type of Attacks	Number of Papers
1	KGA	6
2	LAA	3
3	SOA	2
4	KRA	0

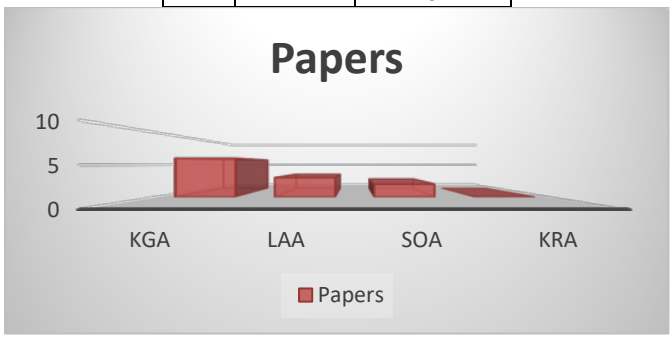

Figure 2: Papers and the type of attack discussed

5 Conclusion

Inferring from this systematic literature reviews, the research is able to classify prominent attacks against encrypted data into four, namely; keyword guessing attacks, key reinstallation attacks, leakage abuse attacks, and selective opening attacks. While many researchers were mainly interested in the penetration testing of these attacks, not much was done in the area of countermeasures. More so, key reinstallation attacks were not discussed specifically, in any of the reputable research papers downloaded for this research work.

6 Recommendations

This paper therefore advice the need for researchers to delve into furthering studies in the area of key reinstallation attacks and finding mitigation measures to all these attacks.

In addition, there is the urgent requirement of defining well stated algorithms that guards the normal flow of activities while encrypted data is in transit online to enable real-time tracking of malicious behaviour online, against encrypted data.

REFERENCES

[1]. Bansal, C., et al., *Keys to the cloud: formal analysis and concrete attacks on encrypted web storage.* International Conference on Principles of Security and Trust 2013. (pp. 126-146). Springer, Berlin, Heidelberg.

[2]. Khan, S., et al., *Network forensics: Review, Taxonomy, and open challenges.* Journal of Network and Computer Applications, 2016. 100(66), 214-235.

[3]. Chaturvedi, S., and R. Sharma, *Securing text & image password using the combinations of persuasive cued click points with improved advanced encryption standard.* Procedia Computer Science, 2015. 45, 418-427.

[4]. Diro, A., and N. Chilamkurti, *Leveraging LSTM Networks for Attack Detection in Fog-to-Things Communications.* IEEE Communications Magazine, 2018. 56(9), 124-130.

[5]. Garcia, D. F., *Performance evaluation of Advanced Encryption Standard (AES)* International Conference on Mathematics and Computers in Sciences and in Industry (MCSI), 2015. pp. 247-252. IEEE.

[6]. Liu, Q., Z., Xu, and Y. Yuan, *High throughput and secure advanced encryption standard on field programmable gate array with fine pipelining and enhanced key expansion.* IET Computers & Digital Techniques, 2015. 9(3), 175-184.

[7]. Liu, X., et al., *Cyber attacks against the economic operations of power systems: A fast solution.* IEEE Transactions on Smart Grid, 2016. 8(2), 1023-1025

[8]. Jiang, P., et al., *Private keyword-search for database systems against insider attacks.* Journal of Computer Science and Technology, 2017. 32(3), 599-617.

[9]. Isah, A. O., et al., *Enhancing AES with Time-Bound and Feedback Artificial Agent Algorithms for Security and Tracking of Multimedia Data on Transition.* International Journal of Cyber-Security and Digital Forensics, 2017. 6(4), 162-179.

[10]. Huang, Q., and H. Li, *An efficient public-key searchable encryption scheme secure against inside keyword guessing attacks.* Information Sciences, 2017. 403, 1-14.

[11]. Boneh, D., X. Boyen, and H. Shacham, *Short group signatures.* In Annual International Cryptology Conference, 2004. (pp. 41-55). Springer, Berlin, Heidelberg.

[12]. Vanhoef, M., and F. Piessens, *Key reinstallation attacks: Forcing nonce reuse in WPA2. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, 2017. (pp. 1313-1328). ACM.

[13]. Huang, Z., et al., *Insight of the protection for data security under selective opening attacks.* Information Sciences, 2017. 412, 223-241.

[14]. Fehr, S., et al., *Encryption schemes secure against chosen-ciphertext selective opening attacks.* In Annual International Conference on the Theory and Applications of Cryptographic Techniques, 2010. pp. 381-402. Springer, Berlin, Heidelberg.

[15]. Grubbs, P., et al., *Leakage-abuse attacks against order-revealing encryption.* In 2017 IEEE Symposium on Security and Privacy (SP), 2017. (pp. 655-672). IEEE.

[16]. Grubbs, P., et al., *Breaking web applications built on top of encrypted data.* In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 2016. pp. 1353-1364. ACM.

[17]. Kellaris, G., et al., *Generic attacks on secure outsourced databases.* In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 2016. pp. 1329-1340. ACM.

[18]. Pouliot, D., and C. V. Wright, *The shadow nemesis: Inference attacks on efficiently deployable, efficiently searchable encryption.* In Proceedings of ACM SIGSAC conference on computer and communications security, 2016. (pp. 1341-1352). ACM.

[19]. Ahmed, A. A., A. S. Sadiq, and M. F. Zolkipli, *Traceback model for identifying sources of distributed attacks in real time.* Security and Communication Networks, 2016. 9(13), 2173-2185.

[20]. Scaife, N., et al., *Cryptolock (and drop it): stopping ransomware attacks on user data.* In 2016 IEEE 36th International Conference on Distributed Computing Systems (ICDCS), 2016. pp. 303-312. IEEE.

[21]. Yakubu, J., et al., *Security challenges in fog-computing environment: a systematic appraisal of current developments.* Journal of Reliable Intelligent Environments, 2019. 1-25.

[22]. Pakniat, N., *Public key encryption with keyword search and keyword guessing attack: a survey.* Proceedings of the 13th International Iranian, 2016. 155, 1-4.

[23]. Andola, N., et al., *Improved secure server-designated public key encryption with keyword search.* In 2017 Conference on Information and Communication Technology (CICT), 2017. pp. 1-6. IEEE.

[24]. Cui, H., et al., *Efficient and expressive keyword search over encrypted data in cloud.* IEEE Transactions on Dependable and Secure Computing, 2016. 15(3), 409-422.

[25]. Lewko, A., A. Sahai, and B. Waters, *Revocation systems with very small private keys.* In 2010 IEEE Symposium on Security and Privacy, 2010. pp. 273-285. IEEE.

[26]. Sun, L., et al., *Secure searchable public key encryption against insider keyword guessing attacks from indistinguishability obfuscation.* Science China Information Sciences, 2018. 61(3), 038106-1.

[27]. Wu, Y., et al., *An efficient searchable encryption against keyword guessing attacks for sharable electronic medical records in cloud-based system.* Journal of medical systems, 2016. 40(12), 258.

[28]. Ma, M., et al., *Certificateless searchable public key encryption scheme for mobile healthcare system.* Computers & Electrical Engineering, 2018. 65, 413-424.

[29]. Wu, T. Y., et al., *Security analysis and enhancement of a certificateless searchable public key encryption scheme for IIoT environments.* IEEE Access, 2019. 7, 49232-49239.

[30]. Rompay, V. C., R. Molva, and M. Önen, *A leakage-abuse attack against multi-user searchable encryption.* Proceedings on Privacy Enhancing Technologies, 2017. 3, 168-178.

[31]. Bost, R., and P. A. Fouque, *Thwarting Leakage Abuse Attacks against Searchable Encryption-A Formal Approach and Applications to Database Padding.* IACR Cryptology ePrint Archive, 2017. 1060.

[32]. Giraud, M., Anzala-Yamajako, A., Bernard, O., & Lafourcade, P. (2017). Practical passive leakage-abuse attacks against symmetric searchable encryption. In *14th International Conference on Security and Cryptography SECRYPT 2017*. SCITEPRESS-Science and Technology Publications.

[33]. Cash, D., et al., *Leakage-abuse attacks against searchable encryption.* In Proceedings of the 22nd ACM SIGSAC conference on computer and communications security, 2015. pp. 668-679. ACM.

[34]. Huang, Z., et al., *Simulation-based selective opening security for receivers under chosen-ciphertext attacks.* Designs, Codes and Cryptography, 2018. 87(6), 1345-1371.

[35]. Hofheinz, D., V. Rao, and D. Wichs, *Standard security does not imply indistinguishability under selective opening.* In Theory of Cryptography Conference, 2016. pp. 121-145. Springer, Berlin, Heidelberg.