







Zero Trust for Intrusion Detection System: A Systematic Literature Review

Abeer Z. Alalmaie^{1,2}^a, Nazar Waheed^{1,3}^b, Mohrah Alalyan³^c, Priyadarsi Nanda¹^d,
Wenjing Jia¹^e and Xiangjian He⁴^f

¹*School of Electrical and Data Engineering, University of Technology Sydney, Sydney, Australia*

²*College of Art and Science, King Khaled University, Rejal Almaa, Abha, Saudi Arabia*

³*College of Art and Science, King Khaled University, Khamis Mushayt, Abha, Saudi Arabia*

⁴*School of Computer Science University of Nottingham Ningbo, China*

Keywords: Zero Trust, Network Intrusion Detection, Anonymization, Trust, Review.

Abstract: Organizations today are facing increasing cybersecurity challenges by moving more services to the cloud and outsourcing Intrusion Detection System (IDS) network monitoring tasks to third-party analysts. Zero Trust models may mitigate these challenges by employing the philosophy of “Never Trust, Always Verify.” However, specific anonymization approaches are required to ensure information integrity while preserving privacy. This paper reviews the existing approaches identified in the literature, compares them, and assesses the privacy-accuracy trade-offs. Plus, we have discussed future research directions and knowledge gaps.


1 INTRODUCTION


Traditionally, enterprise networks have relied on “Implicit Trust” or “Trust but Verify” approaches for traffic control and security. They prevented external intrusions using such mechanisms as firewalls, virtual private networks, and network access controls but treated internal traffic as secure (Heartfield and Loukas, 2016). These approaches are no longer sustainable as organizations are increasingly moving to the cloud, where corporate resources may be accessed by third parties such as customers, analysts, outsourcing partners, and others. With the cloud becoming the new normal, new trust models are needed to ensure a high level of corporate cybersecurity. Zero Trust is a security framework that does not recognize network edges in a traditional sense and does not consider any network areas as trustworthy (Kindervag, 2010). It requires continuous verification of access for all network users at all


times. The key advantage of Zero Trust is that it has a highly adaptable infrastructure that can be combined with the cloud for organizational security improvements (Puthal, et al., 2017).


Zero trust could be especially effective in cases where an Internet Service Provider (ISP) outsources an Intrusion Detection System (IDS) to third-party analysts. Analysts use network tracing to collect information concerning user behavior, packet flows, and other security aspects. However, organizations are concerned about sharing such data due to privacy worries. A number of anonymization approaches have been proposed in the traditional trust model, but none of them offers acceptable levels of privacy and data sharing.


For addressing the privacy concerns associated with sharing sensitive network data in the context of outsourcing IDS to third-party analysts, Machine Learning (ML) and metaheuristic algorithms have played a crucial role. They were employed to


^a <https://orcid.org/0000-0001-7733-8163>

^b <https://orcid.org/0000-0001-5679-5365>

^c <https://orcid.org/0000-0002-1931-8233>

^d <https://orcid.org/0000-0002-5748-155X>

^e <https://orcid.org/0000-0002-0940-3338>

^f <https://orcid.org/0000-0001-8962-540X>

develop advanced data anonymization techniques that not only protect individual identities but also preserve the integrity and utility of the data. These methods can automatically detect and obfuscate sensitive information while still allowing for meaningful analysis of network behavior and security patterns (Tohidi and Rustamov, 2020; Tohidi and Rustamov, 2022).

Furthermore, there is a concern about possible semantic attacks by analysts with access to sensitive corporate data (Figure 1).

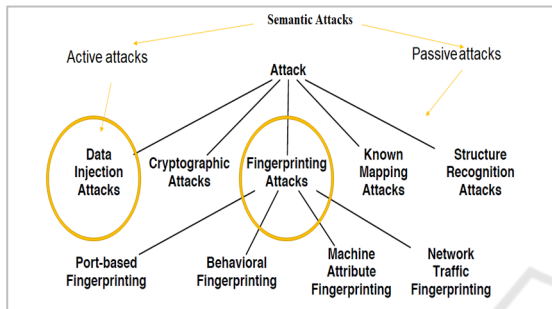


Figure 1: Taxonomy of attacks against network Trace anonymization (Heartfield and Loukas, 2016).

In theory, a Zero-Trust Architecture (ZTA) could resolve this by requiring continuous access verification. However, additional anonymization mechanisms are required to ensure sufficient levels of privacy (needed by organizations) and data availability (needed by analysts). This paper reviews the existing approaches to network trace anonymization under ZTA and identifies the key challenges and possible solutions to those challenges.

A range of zero-trust anonymization tools are currently employed to increase data security in networking tracing environments. Some examples are described below:

1. Anontool is an extendable command line tool based on the anonymization API. It can anonymize both live and stored traffic while allowing users to create anonymization applications and policies according to their needs. They could be applied either to selected single fields or groups of fields. Additionally, Anontool offers a sizeable number of anonymization tools, such as block ciphers, constant/random values, basic mapping functions, regular expression matching and replacement, prefix-preserving anonymization, and various hash functions (Bienias and Kołaczek, 2020).

2. CANINE (Converter and Anonymizer for Investigating NetFlow Events) is a tool that converts and anonymizes NetFlow logs. It exclusively enables one type of NetFlows to operate on data from NetFlows in other formats. Moreover, it supports the anonymization of various fields in multiple ways. CANINE supports Cisco NetFlow V5/V7, which are widely used in the market. CANINE also enables users to select source/destination files, version settings, and fields for anonymization (Li, et al., 2005).
3. FLAIM (Framework for Log Anonymization and Information Management) is a tool based on C++ programming language: it is designed to address anonymizing specific logs supporting multi-level anonymization to balance privacy/security concerns and information quality. A rather flexible in comparison to other applications, FLAIM is designed to share security-related data with other professionals safely (Slagell, et al., 2006).

All these tools, however, have weaknesses by being vulnerable to semantic attacks and requiring heavy sanitization leading to useless data for network analysis. Hence, a tool for preserving accuracy and security is required.

Considering all the mentioned points, a literature review is essential in the context of privacy concerns. It allows researchers and practitioners to gain an understanding of the existing methods, challenges, and advancements related to data anonymization and privacy preservation in network security.

2 RESEARCH METHOD

This study applied a Systematic Literature Review (SLR) approach to data collection and analysis (Tohidi and Dadkhah, 2022). The following research questions were investigated:

RQ1: *what are the existing approaches to for network trace anonymization in the IDS using ZTA?*

RQ2: *what are the key challenges to trace anonymization in such frameworks?*

2.1 Inclusion and Exclusion Criteria

The search was conducted across four major IT databases: ACM Digital Library, IEEE Explore, Elsevier Science Direct, and Springer Link. Given the nature of the study, the keywords used for the search are provided in Table 1. The timeframe for the

studies was between 2010 (introduction of ZTA (Kindervag, 2010)) and 2023. Studies with foci other than Zero Trust, anonymization, and intrusion detection systems were excluded from the review. Only full papers in English were included. To ensure a high level of rigor, only papers from peer-reviewed journals and conferences were considered.

Table 1: Search terms/phrases used to find the existing literature.

Domain	Keywords
Trust	Zero Trust models
Anonymization	Multi-View (MV), Homomorphic Encryption (HE), Computation on Encrypted Databases (CED)
IDSs	Intrusion Detection System (IDS)

2.2 The Search Process

In the search process of the current study, the initial database search using the original keywords returned 731 papers (shown in Table 2). After removing the duplicates and irrelevant studies by using the title and abstract analyses, 46 papers were retained. Then, those were examined deeper, using the quality criteria outlined in Table 3.

Table 2: First iteration of digital library paper statistics.

Digital Library	Keywords: Zero Trust, MV, HE, CED
IEEE Xplore	142
ACM Digital Library	96
(Elsevier) Science Direct	103
SpringerLink	390

Table 3: Quality Criteria.

Quality Criteria	
1	The paper must be a research paper.
2	The paper must have a clearly stated goal.
3	The paper must clearly define the study context.
4	The paper must have a proper framework to meet the study goal(s).
5	The paper must have a rigorous, well-defined approach to data analysis.
6	The paper's findings must be evidence-based.
7	The research in the paper must be validated and/or implemented.

After applying the criteria from Table 3, 15 papers were retained for the final literature analysis and synthesis

3 RESULTS

The analysed studies proposed a number of models for the anonymization of network tracing in ZTA. The models were based on two major approaches: Homomorphic Encryption (HE) and its modifications and the MultiView (MV) approach.

3.1 Homomorphic Encryption

HE is a technique to process encrypted data to protect original information from the third party that processes it (Coppolino, et al., 2021). While using HE protocols for a specific operation, it is required to encrypt the data based on the specific scheme, which only supports the specific operation on that data. Therefore, it is necessary to know the operation in advance while the data are encrypted. Otherwise, each data item should be encrypted through multiple encryption methods to allow multiple operations later, which greatly increases the additional requirement of computational resources. Furthermore, the HE system should also know the type of queries for which operations are to be performed so that an appropriate HE mechanism is selected to encrypt the original data (Jin, et al., 2021).

HE and Intel SGX are used to preserve privacy even while performing different operations on encrypted data in untrusted third-party systems. However, there are some limitations, such as dramatic ciphertext expansion with low bandwidth, the need for off-premises support, being strictly bonded to the hosting server, and limited usable memory. Therefore, the authors in (Coppolino, et al., 2021) proposed the Virtual Secure Enclave (VISE) method that effectively combines HE and Intel SGX techniques to overcome the limitations. VISE does the execution of sensitive HE data on the cloud, where the SGX enclave is attested remotely. Because all computations of the sensitive HE data are performed externally on the cloud, VISE frees the local memory resources.

Since private data must be transferred to the cloud server for large-scale operations, there is a clear need to protect the transferred information so that the original data are not exposed. The authors in (Jin, et al., 2021) proposed a single-server HE mechanism (named CMP-SWHE) using the confused modulo projection theorem to process encrypted data without learning from user data. The designed blind computing scheme uses batch processing which improves computational efficiency while in the process.

Data owners often use encryption for the original data before transferring it to the cloud. Because analyzing encrypted data is challenging, some HE schemes create multikey environments for privacy-preserving data mining. One such scheme was proposed by Pang and Wang (Pang and Wang, 2020) who designed a privacy-preserving association rule mining mechanism to reduce the encrypted data on a cloud server in large-scale shopping malls.

Cheon and Kim (Cheon and Kim, 2015) designed a hybrid mechanism by combining the ElGamal and Goldwasser-Micali schemes that merge public key encryption and SHE for cloud computing environments to reduce the circuit exponentiation at the cost of extra public keys. The proposed mechanism, according to the authors, offers efficient encrypted data computing with lower requirements for storage and bandwidth. Thus, a good balance between the volume of the transmitted ciphertexts and the costs of their conversion is preserved.

Kim et al. in (Kim, et al., 2019) proposed an original algorithm utilizing wildcard pattern matching between encrypted data (i.e., string and keyword) based on leveled FHE and additional encrypted inputs. The researchers proposed original compound query protocols for wildcard search conditions on encrypted databases. The performance evaluation results show that the efficiency of the proposed protocols is comparatively better, but they are not adequate for real-world applications.

Qiu et al. in (Qiu, et al., 2020) designed a scheme using Paillier HE and the data masking technique to perform Privacy-Preserving Linear Regression (PPLR) on the data that were partitioned horizontally in advance. In (Qiu, et al., 2020), two servers operated simultaneously to regress the shared user-submitted data without the need to decipher their contents. The users would submit their data in an encrypted form to a server, and then, two servers collaboratively develop a regression prototype on the shared data without understanding its contents (Figure 2). Data masking techniques, according to the results, offered a higher level of efficiency.

Some FHE schemes are based on multi-key identity to overcome non-adaptive chosen ciphertext attacks (Yuan, et al., 2020). The proposed protocols satisfy the homomorphic (i.e., partially or fully) and compactness properties. Since the mentioned puncturable encryption instantiations are centered on indistinguishability obfuscation, the scheme does not yield practical usability.

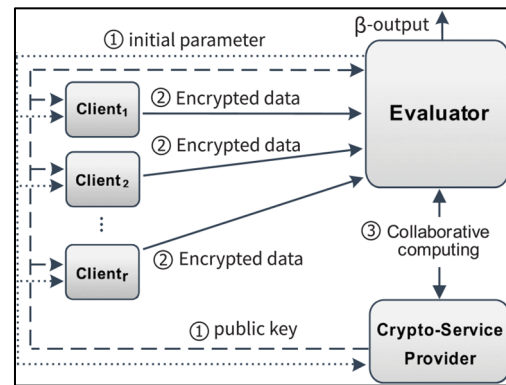


Figure 2: The proposed distributed data analysis system in (Qiu, et al., 2020).

Alagic et al. (Alagic, et al., 2017) designed a protocol for Quantum Fully Homomorphic Encryption with verification (vQFHE) to validate random polynomial-time quantum calculations without involving a client and the server. The proposed scheme also provides correctness, authentication, compactness, and security of verification. It can withstand indistinguishability under a chosen plaintext attack. However, there is an open research question, such as whether any vQFHE schemes exist to confirm quantum computations publicly (while not using the decryption key) or not.

Dyer et al. (Dyer, et al., 2017) proposed HE protocols to do integer arithmetic calculations, which can be used for single-party computation in the cloud securely. In the study, four different schemes were designed to enhance the security level, but the computation overhead is also increased, requiring more computational resources for processing the calculation. The proposed scheme relatively outperforms the related protocols in the computation time of arithmetic operations on encrypted data.

Saha et al. (Saha, et al., 2019) developed what they called an efficient scheme for processing conjunctive and disjunctive private queries over an encrypted database. Their approach applies to lower-depth equality circuits based on the packing methods that result in efficient batch computations. Based on both theoretical analysis and practical evaluations, the proposed schemes were found more efficient in terms of running time and cipher text size (due to the use of a base- N encoding technique) than the existing protocols.

In addition, there is a new technique called Fully Homomorphic encryption based Merkle Tree (FHMT) that aims to Streaming Authenticated Data Structures (SADS) to attain the streaming provable calculation. Therefore, FHMT mostly transfers all

the computation operations to the server, enabling users for no overhead computation. However, the typical FHMT cannot offer the dynamic scenario extensively due to the fixed height. Xu et al. (Xu, et al., 2018) designed a fully dynamic FHMT (DFHMT) mechanism to authenticate an infinite number of data elements while taking less computational overhead. The results of DFHMT demonstrate that the user is required to perform only simple numerical multiplications and additions instead of hash functions while providing the same security as FHMT.

Catalano and Fiore (Catalano and Fiore, 2014) proposed a method to transform a linear HE into a scheme capable of performing second-degree computations on encrypted data. The benefit of the proposed technique, according to the authors, is its light transformation requirement. Specifically, it only requires the message space to be defined as a public ring for arbitrary modeling elements in a uniform manner. As such, full compactness is achieved while performing encrypted data computations on two non-interactive services.

Bellafqira et al. (Bellafqira, et al., 2017) designed a Homomorphic Proxy Re-Encryption protocol (HPRE) to share outsourced cipher text data which were encrypted by applying public keys for remote data operations. The proposed scheme is designed based on encrypted noise (using a secret key) in which the differences between the encrypted noise and data are calculated on the cloud. These differences would be encrypted by the cloud using the delegate’s public key with the subsequent noise removal to reduce computational workload.

Finally, Ahmed et al. (Ahmed and Ogalo, 2019) discussed a Zero Trust model to provide sensitive data access in which the request is granted based on the type of access, user, device, application, and data. They tried to underline some significant developments in the HRM area. They investigated the reasons behind the growing shift from HRM to E-HRM. Plus, their study highlighted an explanation of the features and prospects of E-HRM and its perks compared to traditional HRM works.

3.2 Multiview Approach

Another class of encryption that preserves both the security of the underlying dataset and the accuracy of the analysis is the class of Property Preserving Encryption (PPE). This category of encryption retains certain properties of interest through its scrambling procedure, e.g., distant preserving and prefix preserving. Unfortunately, these encryptions

are shown to be vulnerable to a serious class of attacks called “semantic attacks,” which are designed to collect and extrapolate confidential data about the original datasets through fingerprinting and injection when observing the PPE’s ciphertexts.

Figure 3 illustrates this vulnerability for the class of prefix-preserving encryptions applied to an excerpt of a network trace (borrowed from (Mohammady, et al., 2018)). The two tables demonstrate the original and the prefix preserving anonymized traces. The first step of a semantic attack involves the injection of the network flows corresponding to the first three records in the original trace. Next, the perpetrator is able to use combinations of the unchanged attributes, such as source port and start time, to detect the injected flows. In the third step, the real flows are detected through knowledge extrapolation from the injected flows. In this case, the IP prefix 159.61 shared by the highlighted flows indicates that these flows would share a prefix in the original trace. Accordingly, in the final step of the attack, the perpetrator is able to deanonymize prefixes or IPs for the corresponding flows in the original trace by using the known IPs and the matched prefixes from the injected flows. If the perpetrator is capable of using injection across all subnets, the entire original trace could be successfully deanonymized.

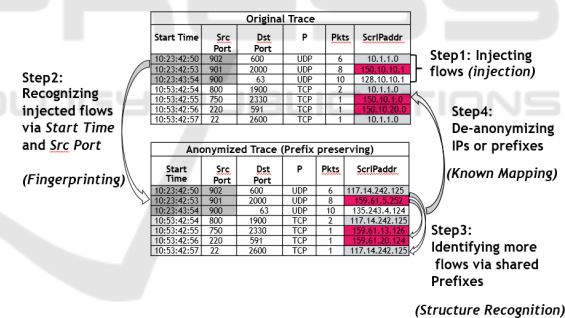


Figure 3: Semantic Attacks: A Toy Example (Mohammady, et al., 2018).

The MV approach was proposed to mitigate this vulnerability while preserving the appealing accuracy of these solutions. The idea behind this approach is the creation of a number of relatively indistinguishable fake views along with the original view making it impossible to distinguish the latter. The only paper using an MV approach was (Mohammady, et al., 2018). The authors described a specific algorithm using CryptoPAn encryption with two distinctive keys, one of which is preserved exclusively by the data owner. After that, the original trace is partitioned using the key which is given to the analyst. The analyst would generate N views based on

Table 4: Summary of Anonymization Approaches and Results.

SLR Papers	Using Zero Trust in outsourcing with IDS monitoring	Anonymization Encryption Approach	Achieves better accuracy	Preserve security	Preserve privacy
(Coppolino, et al., 2021)	No	HE+Intel SGX	Yes	Yes	Yes
(Jin, et al., 2021)	No	Single-server HE	No	Yes	No
(Pang and Wang, 2020)	No	Full HE	No	No	Yes
(Cheon and Kim, 2015)	No	Somewhat HE	No	Yes	No
(Kim, et al., 2019)	No	Full HE	No	Yes	No
(Qiu, et al., 2020)	No	Partial HE	No	Yes	No
(Yuan, et al., 2020)	No	Full HE	No	Yes	No
(Alagic, et al., 2017)	No	Full HE	No	Yes	Yes
(Dyer, et al., 2017)	No	Full HE	No	Yes	No
(Saha, et al., 2019)	No	Full HE	No	Yes	No
(Xu, et al., 2018)	No	Merkle Tree HE	Yes	Yes	No
(Catalano, and Fiore, 2014)	No	Partial HE	Yes	Yes	No
(Bellafqira, et al., 2017)	No	HE Proxy	Yes	Yes	No
(Ahmed, and Ogalo, 2019)	Yes	None	Yes	Yes	No
(Mohammady, et al., 2018)	No	MV	Yes	Yes	No

partitioning, analyze them all, and generate the corresponding reports. However, only by using the second key, the original view could be identified. The experimental results demonstrated that the proposed scheme could expressively decrease the level of information leakage while maintaining comparable utility. Furthermore, since it is required to send only one seed view to the analysts, the proposed solution does not require additional communication overhead. Therefore, the authors concluded that the system offers a better solution for outsourced encrypted data applications to preserve privacy and utility with less computational overhead.

4 DISCUSSIONS

A summary of the anonymization approaches for data tracing identified in the literature as well as the outcomes of their uses is presented in Table 4. The literature review demonstrated that the dominant approach to data anonymization remains homomorphic encryption. Fourteen out of fifteen papers used some kind of HE for network tracing issues. Unfortunately, HE schemes usually suffer from a number of issues, making them impractical architectures for many real-life scenarios. Some common problems with HE models mentioned in the literature were memory consumption and computation time overheads, a lack of expressibility and linkability, as well as integrity issues (Coppolino, et al., 2021; Xu, et al., 2018). Accordingly, few proposed systems managed to achieve the desired levels of privacy and information accuracy. In fact, only (Coppolino, et al., 2021) offered a model that

ensured a relatively high level of data accuracy along with acceptable levels of privacy and security. Unfortunately, the scope of IDS considered in this work is quite limited (to only one intrusion detection task, i.e., Code Injection).

The MV approach, which conceals an accurate view of the original datasets among seemingly indistinguishable fake versions, could be a better solution in this regard. The real view is possible to detect with a unique key, which is generated for the data owner only (Mohammady, et al., 2018). On the one hand, this minimizes the threat of semantic attacks; on the other hand, this ensures that the one analysis based on the true data is highly accurate. Accordingly, this solution does not suffer from the issues inherent to HE as discussed above. However, such systems are still very rare, which means that further research is required to bolster the existing knowledge and ensure the viability of implementing and using MV systems for ZTA IDS.

It is notable that Zero Trust for IDS and AI techniques are closely intertwined as part of a modern cybersecurity approach. Zero Trust emphasizes the principle of continuously verifying the trustworthiness of entities, both inside and outside a network, rather than relying solely on perimeter security. AI techniques, such as machine learning and anomaly detection, play a crucial role within this framework by analyzing vast amounts of data to identify patterns and deviations from normal behavior. In the context of IDS, AI can enhance the accuracy and efficiency of threat detection by learning from historical data, recognizing subtle anomalies, and adapting to evolving cyber threats. By incorporating AI into ZTAs, organizations can

create a dynamic and adaptive defense system that responds proactively to potential intrusions, mitigating risks in real-time and fortifying the security posture of their networks.

As it is seen, the literature review helped identify several significant challenges in using Zero Trust anonymization to enhance the accuracy and security of organizational networks. The following research gaps are identified:

- Research Gap 1: The security issues of outsourcing the IDS tasks to third-party analysts are not identified, i.e., semantic attacks.
- Research Gap 2: Therefore, an effective solution for this scenario has not yet been proposed
- Research Gap 3: The challenges pertaining to designing such a solution are unknown.

5 CONCLUSIONS

The increase in the tendency to apply cloud computing, the Internet of Things, and mobile device use has dissolved traditional network boundaries. Hardened network perimeters alone are no longer effective for providing enterprise security in a world of cloud computing and increasingly sophisticated threats.

The Zero Trust approach combines tight identity-based verification for every person and device attempting to access resources on a private network or the cloud, regardless of whether they are inside or outside the network perimeter. Zero Trust should be considered as a holistic framework rather than be associated with any specific security approach or method. Indeed, it is based on a variety of principles, methods, and ideas of cybersecurity integrated to ensure digital security. Examples include, among others, the prevention of semantic threats, segmenting networks, granular user-access management, and minimization of lateral movement. Zero Trust Architecture could offer an excellent solution to organizations seeking to outsource IDS services to third-party analysts while reducing semantic attack threats. However, the specific anonymization mechanisms ensuring a good balance between privacy and security of such ZTA-based systems are still being explored.

Based on the reviewed literature, the dominant anonymization approaches are based on HE systems which suffer from a number of setbacks, sacrificing either privacy or analytical data accuracy in the process of encryption. MV-based systems may offer a better solution, but they are not sufficiently explored

yet. This review is a part of large-scale research that proposes and evaluates a comprehensive ZTA for the IDS system ZTA-IDS. Such a system could offer a much-needed solution to the edgeless network security where the trade-off between privacy and data utility is minimized.

REFERENCES

- Ahmed, Ammar; Ogalo, Habil Slade. (2019). From HRM to E-HRM: Contemporary developments from scholarly work. *Annals of Contemporary Developments in Management & HR (ACDMHR)*, 1, 1-6.
- Alagic, Gorjan; Dulek, Yfke; Schaffner, Christian; Speelman, Florian. (2017). Quantum Fully Homomorphic Encryption With Verification. arXiv:1708.09156, Cornell University.
- Bellafqira, Reda; Coatrieux, Gouenou; Bousslimi, Dalel; Quellec, Gwenole; Cozic, Michel;. (2017). Proxy Re-Encryption Based on Homomorphic Encryption. *The 33rd Annual Computer Security Applications Conference*. Seoul, Korea.
- Bienias, P., Warzyński, A., & Kołaczek, G. (2020). Application and preliminary evaluation of Anontool applied in the anomaly detection module. *IEEE 29th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE)* (pp. 119-123). Bayonne: IEEE. doi:10.1109/WETICE49692.2020.00031
- Catalano, Dario; Fiore, Dario;. (2014). Boosting Linearly-Homomorphic Encryption to Evaluate Degree-2 Functions on Encrypted Data. *cryptoeprint:2014/813*. Retrieved from <https://ia.cr/2014/813>
- Cheon, Jung Hee; Kim, Jinsu. (2015). A Hybrid Scheme of Public-Key Encryption and Somewhat Homomorphic Encryption. *IEEE Transactions on Information Forensics and Security*, 10(5), 1052 - 1063.
- Coppolino, L., D'Antonio, S., Formicola, V., Mazzeo, G., & Romano, L. (2021). VISE: Combining Intel SGX and Homomorphic Encryption for Cloud Industrial Control Systems. *IEEE Transactions on Computers*, 70(5), 711 - 724.
- Dyer, James; Dyer, Martin; Xu, Jie. (2017). Practical Homomorphic Encryption Over the Integers. arXiv:1702.07588, Cornell University.
- Heartfield, Ryan; Loukas, George. (2016). A Taxonomy of Attacks and a Survey of Defence Mechanisms for Semantic Social Engineering Attacks. *ACM Computing Surveys*, 48(3), 1–39. doi:10.1145/2835375
- Jin, Xin; Zhang, Hongyu; Li, Xiaodong; Yu, Haoyang; Liu, Beisheng; Xie, Shujiang; Singh, Amit Kumar; Li, Yujie. (2021). Confused-Modulo-Projection-Based Somewhat Homomorphic Encryption—Cryptosystem, Library, and Applications on Secure Smart Cities. *IEEE Internet of Things Journal*, 8(8), 6324-6336.
- Kim, Myungsun; Lee, Hyung Tae; Ling, San; Meng Tan, Benjamin Hong; Wang, Huaxiong. (2019). Private Compound Wildcard Queries Using Fully

- Homomorphic Encryption. *IEEE Transactions on Dependable and Secure Computing*, 16(5), 743-756.
- Kindervag, J. (2010). *Build Security Into Your Network's DNA: The Zero Trust Network Architecture*. For Security & Risk Professionals, Forrester Research.
- Li, Y., Slagell, A., Luo, K., & Yurcik, W. (2005). CANINE: A Combined Conversion and Anonymization Tool for Processing NetFlows for Security. *International Conference on Telecommunication Systems, Modeling and Analysis*. Dallas.
- Mohammady, Meisam; Wang, Lingyu; Hong, Yuan; Louafi, Habib; Porzandi, Makan; Debbabi, Mourad, (2018). Preserving Both Privacy and Utility in Network Trace Anonymization. *ACM SIGSAC Conference on Computer and Communications Security* (pp. 459–474). Toronto, Canada: Association for Computing Machinery. doi:https://doi.org/10.1145/3243734.3243809
- Pang, Hongping; Wang, Baocang. (2020). Privacy-Preserving Association Rule Mining Using Homomorphic Encryption in a Multikey Environment. *IEEE Systems Journal*, 99, 1-11. doi:10.1109/JSYST.2020.3001316
- Puthal, D.; Mohanty, S.P.; Nanda, P.; Choppali, U. (2017). Building security perimeters to protect network systems against cyber threats [future directions]. *IEEE Consumer Electronics Magazine*, 6(4), 24- 27.
- Qiu, Guowei; Gui, Xiaolin; Zhao, Yingliang. (2020). Privacy-Preserving Linear Regression on Distributed Data by Homomorphic Encryption and Data Masking. *IEEE Access*, 8, 107601-107613.
- Saha, Tushar Kanti; Rathee, Mayank; Koshiha, Takeshi. (2019). Efficient private database queries using ring-LWE somewhat homomorphic encryption. *Journal of Information Security and Applications*, 49.
- Slagell, A., Lakkaraju, K., & Luo, K. (2006). FLAIM: A Multilevel Anonymization Framework for Computer and Network Logs. *Computing Research Repository - CORR*, (pp. 63-77).
- Tohidi, Nasim; Dadkhah, Chitra. (2022). A Short Review of Abstract Meaning Representation Applications. *Journal of Modeling & Simulation in Electrical & Electronics Engineering*, 2(3), 1-9.
- Tohidi, Nasim; Rustamov, Rustam B. (2020). A review of the machine learning in gis for megacities application. In *Geographic Information Systems in Geospatial Intelligence* (pp. 29-53). London: IntechOpen.
- Tohidi, Nasim; Rustamov, Rustam B. (2022). Short Overview of Advanced Metaheuristic Methods. *International Journal on Technical and Physical Problems of Engineering (IJTPE)*, 14(51), 84-97.
- Xu, Jian; Wei, Laiwen; Zhang, Yu; Wang, Andi; Zhou, Fucai; Gao, Chong-zhi;. (2018). Dynamic Fully Homomorphic encryption-based Merkle Tree for lightweight streaming authenticated data structures. *Journal of Network and Computer Applications*, 107, 113-124.
- Yuan, Minghao; Wang, Dongdong; Zhang, Feng; Wang, Shenqing; Ji, Shan; Ren, Yongjun. (2020). An Examination of Multi-Key Fully Homomorphic Encryption and Its Applications. *Mathematics*, 10(24), 1-20.