Mitigating the Risks of Whistleblowing
An Approach Using Distributed System Technologies

Ali Habbabeh[1], Petra Maria Asprion[1], and Bettina Schneider[1]

[1] University of Applied Sciences Northwestern Switzerland, Basel, Switzerland

ali.habbabeh@fhnw.ch
petra.asprion@fhnw.ch
bettina.schneider@fhnw.ch

Abstract. Whistleblowing is an effective tool to fight corruption and expose wrongdoing in governments and corporations. Insiders who are willing to report misconduct, called whistleblowers, often seek to reach a recipient who can disseminate the relevant information to the public. However, whistleblowers often face many challenges to protect themselves from retaliation when using the existing (centralized) whistleblowing platforms. This study discusses several associated risks of whistleblowing when communicating with third parties using webforms of newspapers, trusted organizations like WikiLeaks, or whistleblowing software like GlobaLeaks or SecureDrop. Then, this study proposes an outlook to a solution using decentralized systems to mitigate these risks using Blockchain, Smart Contracts, Distributed File Synchronization and Sharing (DFSS), and Distributed Domain Name Systems (DDNS).

Keywords: Whistleblowing, Blockchain, Smart Contracts

1 Introduction

By all indications, the topic of whistleblowing has been gaining extensive media attention since the financial crisis in 2008, which ignited a crackdown on the corruption of institutions [1]. However, some whistleblowers have also become discouraged by the negative association with the term [2], although numerous studies show that whistleblowers have often revealed misconduct of public interest [3]. Therefore, researchers like [3] argue that we - the community of citizens - must protect whistleblowers. Additionally, some researchers, such as [1], claim that, although not perfect, we should reward whistleblowers financially to incentivize them to speak out to fight corruption [1]. Despite that, many European countries, for example Germany or Switzerland, do not offer monetary rewards or even sufficient protection for whistleblowers. Recently, the Swiss parliament rejected a bill, for the second time, to provide whistleblowers with protection, which many Swiss whistleblowers were longing for, especially after some lost their jobs and others were sentenced to prison [4].

As a baseline, this study investigates the existing (online) whistleblowing platforms. In particular, it analyzes their security risks on whistleblowers' anonymity. As main contribution, this study suggests improvements that tackle the challenge of protecting the identity of whistleblowers and rewarding them at the same time while being anonymous. To achieve the goal of protecting and rewarding whistleblowers without revealing their identity, newer distributed systems technologies such as Blockchain, Smart Contracts, Distributed File Synchronization and Sharing (DFSS), and Distributed Domain Name Systems (DDNS) are investigated.

As methodological framework, the Design Science Research (DSR) approach by [5] was followed. Widely applied in Information Systems research, DSR aims at generating an artifact to accomplish the goal of solving a problem efficiently and effectively [6]. The framework ensures a strong relationship between the research work, the environment and the knowledge base. To gather and investigate the existing knowledge, a literature review on whistleblowing was conducted applying the criteria suggested by [6]. First, keywords such as 'risks of whistleblowing', 'problems of whistleblowing', or 'safe whistleblowing' were used. In a second step, further keywords e.g., 'whistleblowing technologies', 'platforms for whistleblowing', or 'whistleblowing' combined with 'newspapers' enabled identification of existing platforms. Academic literature (peer-reviewed journals, books) were in focus, enriched by grey literature.

2 Whistleblowing

Whistleblowing is an action of a former or current member/group of members of an organization who discloses information concerning illegal or immoral conduct of its employers to other entities that are able to act on this information [7]. Although widely accepted and cited in many papers, some academics regard this definition to be problematic, as it takes into account both internal and external disclosure of information of being a whistleblowing activity [8]. For instance, [9] considers an information leak as whistleblowing only when it is leaked to external parties, such as the media or government officials [9]. By contrast, [7] argue that internal whistleblowing could be a good measure to correct the wrongdoing within an organization and leading to upper management dealing with the illegal/immoral activity without disclosing this to the public. This study considers whistleblowing to consist of five technically essential steps referred to as 'whistleblowing process' [8-10]:

I. A whistleblower reports misconduct anonymously.
II. Then, a medium of whistleblowing receives the report.
III. Later an interested party receives the report.
IV. Afterward, a channel of communication between the whistleblower and the interested party is facilitated.
V. Finally, a payment service for the whistleblower is enabled while the whistleblower still being anonymous.

2.1 Existing Whistleblowing Platforms

In this section, we review the existing most widely known whistleblowing platforms. Even though hotlines, case management software, and emails can be used as solutions, we will only consider platforms that (try to) preserve, the whistleblower's privacy from a technical perspective. For that reason, we look at:

1) Client/Server web forms. Use case: Local newspapers in Switzerland.
2) Well-known whistleblowing organizations. Use case: *WikiLeaks*.
3) Whistleblowing open-source software. Use cases: SecureDrop and GlobaLeaks.

2.2 Use Case 1: Whistleblowing through Web Forms

One way to 'blow the whistle' is to contact a journalist of a local newspaper and communicate information about the witnessed wrongdoing. Some newspapers, depending on the budget and interest, offer a website 'as a service' for whistleblowers to contact them while others do not. Many Swiss local newspapers rely on contact forms to receive tips and offer no clear way to communicate with them other than that. For example, in Switzerland, eleven local newspapers were examined or contacted to investigate their whistleblowing tips-receiving process (see Table 1). None of the investigated newspapers had a sufficiently secure method. Instead, newspapers offer a web form − usually a named contact form − that can be used for any communication purpose.

Table 1. Swiss newspapers whistleblowing tips-receiving methods (examples).

Newspaper	Whistleblowing Method
20 Minuten	Community: https://www.20min.ch/community/leser_reporter/ People can upload photos or videos with a limited short message
Blick	No method was found.
Tagesanzeiger	contact form: https://abo.tagesanzeiger.ch/tamstorefront/contact
Neue Zürcher Zeitung	contact form: https://abo.nzz.ch/kontakt/
Watson	contacts found: https://www.watson.ch/u/impressum
Le Matin	contacts found: https://www.lematin.ch/services/divers/Impressum/story/24227737
Basler Zeitung	contact form: https://abo.bazonline.ch/tamstorefront/contact
Le Temps	contact form: https://www.letemps.ch/contact
SWI- Swiss Info	contact form: https://www.swissinfo.ch/contact/ger/42718408
Berner Zeitung	contact form: https://abo.bernerzeitung.ch/tamstorefront/contact

2.3 Use Case 2: Whistleblowing Organizations: WikiLeaks

WikiLeaks is an international non-profit organization publishing classified documents provided by whistleblowers to their platform [10]. *WikiLeaks* was founded in 2006 and caught the attention the next year when it released the manuals of Guantanamo's corrections officers' manuals. Although *WikiLeaks* started as an international

organization that collaborated with whistleblowers worldwide, over time it shifted its focus to the United States only [11].

2.4 Use Case 3: Whistleblowing Software: SecureDrop and GlobaLeaks

Currently, two well-known open-source software projects to support whistleblowing exist: *GlobaLeaks* [12] and *SecureDrop* [13]. *SecureDrop* is an application organizations can choose and install to receive documents from anonymous sources over the internet [14]. *SecureDrop*'s development started in 2013 under the name *DeadDrop* in the period when *WikiLeaks* file submission software was down [14]. It was later renamed to *SecureDrop* after the 'Freedom of the Press Foundation' took over the management [15]. Unlike *SecureDrop*, *GlobaLeaks* enables non-tech-savvies to set up a secure whistleblowing system, which is considered by some researchers to be more user-friendly compared to *SecureDrop* and simpler in terms of architecture (e.g., [16]). *GlobaLeaks* has many instances that operate separately. Thus, it is not centralized in the sense that every node has its own documents, and taking down one node does not affect the others [17].

3 Risks of Whistleblowing

This section discusses the risks whistleblowers face when leaking information via existing whistleblowing platforms. The risks were identified by means of a systematic literature review described in section 1. Collected results were evaluated as recommended by [6], and lead to a categorization summarized in Table 2.

Table 2. Risks of whistleblowing

Risk	Description
R1: Anonymity of Whistleblowers	Whistleblowers' identity can be revealed through several methods, which can lead to retaliation against them.
R2: Integrity of Information	Disclosures of whistleblowers can be altered, which can lead to false information being published.
R3: Confidentiality of Disclosures	Hackers can eavesdrop on the communication between whistleblowers and receivers like journalists.
R4: Availability of Service	A platform can be out of service due to a DDoS attack on its servers, which prevents whistleblowers from using it.
Other Risks:	Usability, the authenticity of the information, plausible deniability of whistleblowers.

3.1 R1: Anonymity of Whistleblowers

Anonymity is defined as an assurance that a subject's identity cannot be inferred from exposed data [18]. Even though there exist cases, where whistleblowers open up to the public, revealing identity is generally not desirable. Stiff reprisal and retaliation

from the accused wrongdoers could be the consequences making anonymity a vital requirement.

Anonymity when using web forms: Newspapers

As described in section 2.2, most investigated newspapers offer email channel, submission forms, or similar web services for whistleblowers to contact them. Most of these online services are part of a client/server architecture entailing several anonymity risks. Examples are WebRTC (IP) leak, DNS leak [19], unauthorized eavesdropping [20], or IP spoofing [21]. The nature of these risks is discussed extensively in the literature (e.g., [22]). Another aspect is revealing the communication between whistleblowers and the journalist from the intended newspaper. If this communication takes place using an email service, the security of this communication depends on the safety of the email server. According to an interview with an investigative journalist, most journalists use mobile applications such as *Signal* or *WhatsApp* to communicate with whistleblowers. These apps incorporate end-to-end encryption but require the whistleblower's phone number, which could lead to subject identification [23].

Anonymity in whistleblowing organizations: WikiLeaks

WikiLeaks offers an onion address to its users and accepts leaks only through their onion address, which means users are forced to use a so-called *Tor* browser [24]. The problem of onion addresses is that they are not readable by humans. Consequently, users usually access *wikileaks.org* to get a copy of the onion address. This step presents them with the risk of being identified in case anonymization measures such as *Tor* are not used. *WikiLeaks* does not encrypt the files whistleblowers submit on the client-side, but claims the data encryption to happen on server-side. Yet since the *WikiLeaks* platform is not open-source, it is not possible to confirm the encryption. A malicious observer out of the whistleblower network, the service provider, could potentially eavesdrop on the whistleblower and access the data before it reaches the server (eavesdropping attack) [25]. Moreover, whistleblowers must trust the *WikiLeaks* server admins to handle their files with specific care to ensure the anonymity of their identity. This means some sort of a trust level is required in the *WikiLeaks* setup.

The anonymity of Whistleblowing software: SecureDrop & GlobaLeaks

Both solutions offer server-side encryption only, which protects the data from a potential breach but not from a possible malicious system administrator [26], [27]. *SecureDrop* can be considered to offer superior anonymity due to its secure methods in handling whistleblowing cases, in which journalists are required to decrypt files using a machine that is not connected to the internet [14].

3.2 R2: Integrity of Information

Information integrity is the assurance that information has not been altered throughout its whole lifecycle by an unauthorized party [28]. In a whistleblowing context, this means that the disclosures of whistleblowers do not get modified without their

knowledge and acceptance [23]. Integrity can be compromised by attacks such as *Salami*, *Data diddling*, *Man-in-the-middle*, or *Session hijacking attacks* [29].

Integrity when using web forms: Newspapers

In the surveyed newspapers (see Table 1), usage of *HyperText Transfer Protocol Secure* (HTTPs) − an extension and more secure version of the older *HyperText Transfer Protocol* (HTTP) − was observed to be the common case [30]. This way, in theory, the information whistleblowers provide by submitting online forms can be preserved and stored unaltered, assuming none of the previously mentioned attacks are executed.

Integrity in whistleblowing organizations: WikiLeaks

WikiLeaks employs *Tor* for its submission form. According to [31], the file-upload system applied by *WikiLeaks* protects the submission of whistleblowers from any network eavesdropping [31]. However, [32] argues that there is no way for readers to assure that the materials released by *WikiLeaks* are unaltered. According to [32], readers could nevertheless trust the platform. This claim is based on actions taken by *WikiLeaks* in the past when they refused to delete sensitive data of whistleblowers' disclosures.

Integrity of whistleblowing software: SecureDrop & GlobaLeaks

Similar to *WikiLeaks*, both software employ *Tor* and HTTPs to receive disclosures from whistleblowers [33]. Nevertheless, according to *SecureDrop*'s documentation [33], assumptions are made to guarantee safety. As an example it is stated: "The admin and the journalist act reasonably and in good faith." [33]. This claim is hard to ensure.

3.3 R3: Confidentiality of Disclosures

Confidentiality in a data context is an attribute that means information must not be made available or disclosed to unauthorized or unintentional parties in a readable format [34]. According to [35], if information confidentiality concerns are low, this information is considered public or unthreatening if revealed beyond the intended audience. Regarding whistleblowing, the disclosures, and the communication messages between whistleblowers and third parties, i.e., the potential publishers, must be confidential in order to avoid exposure of identity information.

Confidentiality when using web forms: Newspapers

When whistleblowers submit documents to a newspaper using a web form, the confidentiality property can be violated in case the system admin, as an example, reads the content of the submission. Even though it is safe to assume that whistleblowers are aiming at making their information public, and therefore do not have confidentiality requirements for their submission [23], some disclosures require a specific publisher to gain access to the information first. However, if a web form is used to transmit the leak, confidentiality could be jeopardized in case of successful attacks, such as the *Man-in-the-middle*, *packet sniffing*, or *password attack* [36].

Confidentiality in whistleblowing organizations: WikiLeaks

Whistleblowers submitting disclosures to *WikiLeaks* have to expect that all of their journalists get access to the transmitted data [37]. A whistleblower cannot declare to

which employee of *WikiLeaks* the case is assigned. Consequently, it is assumed that whistleblowers are indifferent to whom handles that case inside *WikiLeaks* organization since they technically lose ownership of the case when they hand it in. Therefore, the confidentiality property is solely dependent on the reliability of the submission system that *WikiLeaks* offer.

The Confidentiality of Whistleblowing software: SecureDrop & GlobaLeaks

As a means to ensure confidentiality, *SecureDrop* recommends, but not enforces, the *Tails* operation system for any hardware journalists use to connect to the *SecureDrop* server [33]. The *Airgrapped Area* by contrast applies the use of *Tails* to secure the decryption process of submissions that were encrypted on the server-side. Moreover, whistleblowers can communicate with the recipients using the same protocol [33]. Thus, it can be considered that *SecureDrop* guarantees that the transmitted data, both submissions, and communications, are only read by the party with which the whistleblower intended to communicate. The backend solution of *GlobaLeaks* enables the whistleblowers to communicate with the recipients of their submission using comments, which are visible to all parties in that context, i.e., both the whistleblower and the recipients [38]. The interaction and communication of the whistleblowers can take place anonymously thanks to the *Tor* service that *GlobaLeaks* employs.

3.4 R4: Availability of Service

Availability is "the degree to which a system, subsystem or equipment is in a specified operable and committable state at the start of a mission when the mission is called for a random time" [39]. In other words, unavailability is the probability of the inability of a user to access specific data or resources. Since whistleblowing can be time-sensitive, platforms must be available at any time.

Availability when using web forms: use case Newspapers

The availability of a webform is connected to the availability of the underlying infrastructure. One of the most well-known attacks on the availability of a website is a *Denial-of-Service* (DoS) or the more threatening version of it, the *Distributed DoS* attack (DDoS) [40]. In general, large, well-known newspapers utilizing client/server architecture might be appealing targets for attackers.

Availability in whistleblowing organizations: WikiLeaks

WikiLeaks has a long history of DDos attacks. The first documented attack was in November 2010 [41], followed by another one in December 2010 when *Anonymous* hacktivists attacked *WikiLeaks* using a DDos attack [42]. Later in 2012, *WikiLeaks* suffered from multiple DDos attacks that lasted at some point up to four days [43].

The Availability of Whistleblowing software: SecureDrop & GlobaLeaks

In their documentation, *GlobaLeaks* states that the software has resiliency to avoid application and database DoS [26]. *GlobaLeaks* achieves that by putting limits on the automation of operation and enforcing human interaction [26]. However, some of these measures are browser-based, which means that browser-independent attacks can still

compromise availability. For example, in their audit security audit, [44] found that uploading a large file is prevented only from the browser side, and no mechanisms were found to stop attacks that are browser-independent. In the most recent security impact assessment of *SecureDrop* conducted by a third party, no significant threats were found regarding availability [45]. However, *SecureDrop* states that an attacker could generally compromise the availability of a server by uploading a large number of documents using different identities [33].

4 Potential Mitigation Solution

One potential improvement to the existing whistleblowing platforms would be integrating distributed systems technologies such as Blockchain and Smart Contracts. Their specific characteristics can help to overcome the risks of whistleblowing mentioned in Table 2. For example, Blockchain offers an immutable decentralized ledger stored on several nodes [46]. This can be utilized to prevent government censorship. The decentralized architecture allows for eliminating the need for a governing third party, which implies an unbiased administration of the software running on top of a Blockchain [47]. Moreover, due to its distributed architecture, Blockchain technology can prevent DDos attacks [48]. In addition, Blockchain addresses are pseudonymous, which means that users' accounts are not linked to their personally identifying information by nature [49]. The pseudonymous addresses can be employed to provide whistleblowers with the required privacy. To enable users to interact with the Blockchain, Smart Contracts are to be deployed to facilitate the communication and transactions between whistleblowers and other parties like journalists. The code of Smart Contracts in Ethereum is public by nature and, depending on its purpose, can facilitate buying and selling activities using cryptocurrencies, which are digital currencies that use encryption to regulate fund transactions [50]. Cryptocurrencies can be employed to enable rewarding whistleblowers without revealing their identities.

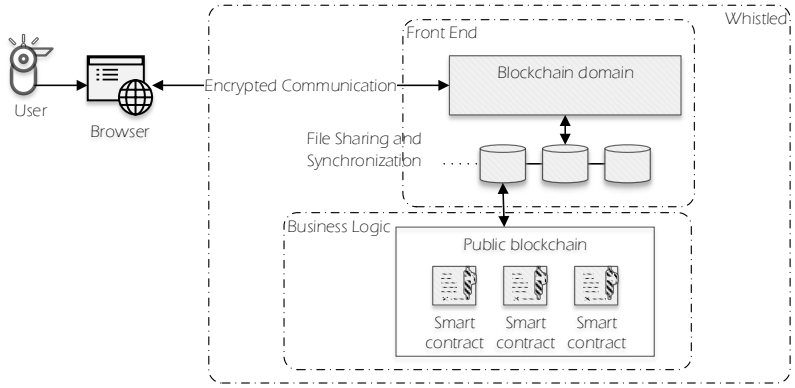

Fig. 1. The landscape of a decentralized whistleblowing prototype

Figure 1 illustrates a high-level decentralized landscape of our suggested solution named *Whistled*. To enable whistleblowers to interact with Smart Contracts familiarly, a frontend and website are needed. A domain is necessary to host this website. However, accessing the frontend using a traditional domain name bought from a domain provider can compromise the decentralization of the whistleblowing platform. This is a risk since a domain provider can take down any domain when requested by an authority [51]. Therefore, a decentralized domain name, also known as a Blockchain domain, is recommended to control the frontend of the *Whistled* platform. The content of a Blockchain domain resides on a decentralized file system known as IPFS, which is a DFSS. IPFS is a peer-to-peer network that offers redundancy and, just like Blockchain, is decentralized [52]. Thus, the content that whistleblowers provide, and the content of the frontend of the platform will be stored on IPFS to prevent censorship and improve the continuity factor of the platform. Although leaks are published, the files submitted by whistleblowers will be encrypted, making them unreadable for unauthorized parties.

5 Conclusion

This study has investigated improving the whistleblowing process by employing a combination of distributed system technologies. Multiple risks of whistleblowing platforms − *WikiLeaks*, *SecureDrop*, *GlobaLeaks* − and of newspapers' whistleblowing offerings were identified and analyzed. These risks include compromising the anonymity of whistleblowers and, in the least, the integrity, confidentiality, availability of information provided. To mitigate these risks, a decentralized platform has been suggested, in which Smart Contracts, Blockchain domains, and file sharing and synchronization play a role to prevent censorship, increase privacy, and guarantee continuity.

To realize the prototype based on Blockchain technology and Smart Contracts, a detailed architecture must be created based on technology selections, where the prototype elements are divided into business logic and frontend realization. Blockchain wallets can be used as a zero-knowledge identification tool to anonymize whistleblowers and transfer tokens between them and third parties. In addition, Smart Contracts can enable the implementation of the derived use cases such as submitting, viewing, receiving of whistleblowers' cases, and rewarding whistleblowers by transferring tokens to them when needed.

References

[1] B. McLannahan, "Best way to encourage whistleblowers? Reward them | Financial Times," 2019. https://www.ft.com/content/cac4c994-3f24-11e9-9bee-efab61506f44 (accessed Sep. 05, 2020).

[2] T. Miethe, *Whistleblowing at work: Tough choices in exposing fraud, waste, and abuse on the job*. Routledge, 2019.

[3] W. Vandekerckhove, *Whistleblowing and organizational social responsibility: A global assessment*. Routledge, 2016.

[4] SDA, "Parlament lässt Whistleblower im Ungewissen," 2020.

https://www.nau.ch/politik/bundeshaus/parlament-lasst-whistleblower-im-ungewissen-65673189?fbclid=IwAR0OGgrVTiI4-wmhbDpZ0t2-AWJE87uM4jbgjf8b9h5800GAM3WUOxfg4f0 (accessed Sep. 03, 2020).

[5] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design Science in Information Systems Research," *Des. Sci. IS Res. MIS Q.*, vol. 28, no. 1, pp. 75–105, 2004, Accessed: May 15, 2018. [Online]. Available: https://pdfs.semanticscholar.org/fa72/91f2073cb6fdbdd7c2213bf6d776d0ab411c.pdf.

[6] M. Saunders, P. Lewis, and A. Thornhill, *Research Methods for Business Students- 7th Edition*. 2015.

[7] J. P. Near and M. P. Miceli, "Organizational Dissidence: The Case of Whistle-Blowing*," 1985.

[8] G. King, "The Implications of an Organization's Structure on Whistleblowing," *J. Bus. Ethics*, no. 4, 1999, Accessed: Oct. 26, 2019. [Online]. Available: https://link.springer.com/content/pdf/10.1023%2FA%3A1006028417000.pdf.

[9] D. Farrell and J. C. Petersen, "Patterns of political behavior in organization," *Acad. Manag. Rev.*, vol. 7, no. 3, pp. 403–412, 1982.

[10] WikiLeaks, "WikiLeaks: What is WikiLeaks," *03 November 2015*, 2015. https://wikileaks.org/What-is-WikiLeaks.html (accessed Aug. 30, 2020).

[11] T. E. Times, "Controversy strikes - Five things to know about WikiLeaks," 2019. https://economictimes.indiatimes.com/news/international/world-news/five-things-to-know-about-wikileaks/controversy-strikes/slideshow/68832511.cms (accessed Nov. 24, 2019).

[12] GlobaLeaks, "GlobaLeaks | The OpenSource Whistleblowing Software." https://www.globaleaks.org/ (accessed Apr. 04, 2020).

[13] SecureDrop, "Share and accept documents securely - SecureDrop." https://securedrop.org/ (accessed Sep. 04, 2020).

[14] C. Berret, "Guide to SecureDrop," 2016, doi: 10.7916/D84178B2.

[15] Ssteele, "Tor At The Heart: SecureDrop," 2016. https://blog.torproject.org/tor-heart-securedrop (accessed Apr. 04, 2020).

[16] I. Zakia, A. H. Fatahillah, N. R. Syambas, A. Setiawati, and H. Mubarok, "Aspiration and complaint system: From literature survey to implementation," in *2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA)*, 2017, pp. 1–6.

[17] K. Thiel, *JULIAN ASSANGE : founder of wikileaks.* [Place of publication not identified]: CAVENDISH SQUARE, 2018.

[18] S. Motahari, S. G. Ziavras, and Q. Jones, "Online anonymity protection in computer-mediated communication," *IEEE Trans. Inf. Forensics Secur.*, vol. 5, no. 3, pp. 570–580, 2010.

[19] A. Hochstadt, "What's the difference between a MAC address and IP address?," 2018. https://www.vpnmentor.com/blog/whats-difference-dns-ip-leaks-stop/ (accessed Apr. 18, 2020).

[20] G. S. Miliefsky, "System and method for detecting, alerting and blocking data leakage, eavesdropping and spyware." Google Patents, May 22, 2014.

[21] A. Yaar, A. Perrig, and D. Song, "StackPi: New packet marking and filtering mechanisms for DDoS and IP spoofing defense," *IEEE J. Sel. Areas Commun.*, vol. 24,

no. 10, pp. 1853–1863, 2006.
[22] N. Ketcha, “Financial Institution Letters Risks Involving Client/Server Computer Systems,” 2011. Accessed: Apr. 18, 2020. [Online]. Available: https://ithandbook.ffiec.gov/media/resources/3406/fdi-fil-82-96-risks_involv_client_server_comp_sys.pdf.
[23] M. Hassan, “Personal Interview with an Investigative Journalist M. Hassan,” 2020, [Online]. Available: https://arij18.arij.net/speakers/majdolin-hasan/.
[24] WikiLeaks, “WikiLeaks.” https://wikileaks.org/ (accessed Mar. 26, 2020).
[25] S. K. Das, K. Kant, and N. Zhang, *Handbook on securing cyber-physical critical infrastructure*. Elsevier, 2012.
[26] GlobaLeaks, “Application security — GlobaLeaks 4 documentation,” 2020. https://docs.globaleaks.org/en/devel/security/ApplicationSecurity.html?highlight=DOS#dos-resiliency-approach (accessed May 09, 2020).
[27] SecureDrop, “Directory - SecureDrop.” https://securedrop.org/directory/ (accessed Apr. 04, 2020).
[28] S. K. Jain, “Strategy to avoid data integrity issues in pharmaceutical industry,” *Pharma Innov.*, vol. 6, no. 2, Part B, p. 110, 2017.
[29] M. S. Hossain, A. Paul, M. H. Islam, and M. Atiquzzaman, “Survey of the Protection Mechanisms to the SSL-based Session Hijacking Attacks.,” *Netw. Protoc. Algorithms*, vol. 10, no. 1, pp. 83–108, 2018.
[30] A. P. Felt, R. Barnes, A. King, C. Palmer, C. Bentzel, and P. Tabriz, “Measuring {HTTPS} Adoption on the Web,” in *26th {USENIX} Security Symposium ({USENIX} Security 17)*, 2017, pp. 1323–1338.
[31] A. Greenberg, “WikiLeaks Finally Brings Back Its Submission System for Your Secrets | WIRED,” 2015. https://www.wired.com/2015/05/wikileaks-finally-brings-back-submission-system-secrets/ (accessed Sep. 01, 2020).
[32] P. Holland, “What is WikiLeaks? - CNET,” 2017. https://www.cnet.com/how-to/what-is-wikileaks/ (accessed Sep. 20, 2020).
[33] SecureDrop, “Overview — SecureDrop 1.2.2 documentation,” 2019. https://docs.securedrop.org/en/latest/overview.html (accessed Apr. 04, 2020).
[34] A. L. Franzoni, C. Cárdenas, and A. Almazan, “Using Blockchain to Store Teachers’ Certification in Basic Education in Mexico,” in *2019 IEEE 19th International Conference on Advanced Learning Technologies (ICALT)*, 2019, vol. 2161, pp. 217–218.
[35] University of Deleware, “Managing data confidentiality,” *Secure UD*, 2018. https://www1.udel.edu/security/data/confidentiality.html (accessed Apr. 29, 2020).
[36] M. Raza, M. Iqbal, M. Sharif, and W. Haider, “A survey of password attacks and comparative analysis on methods for secure authentication,” *World Appl. Sci. J.*, vol. 19, no. 4, pp. 439–444, 2012.
[37] WikiLeaks, “how to send your submission to Wikileaks.” https://warlogs.wikileaks.org/media/submissions.html (accessed Sep. 02, 2020).
[38] GlobaLeaks, “Architecture · globaleaks/GlobaLeaks Wiki,” 2019. https://github.com/globaleaks/GlobaLeaks/wiki/Architecture (accessed May 02, 2020).
[39] S. Rajesh and A. Chandrasekar, “Esteemed software patterns for banking system,” *Cluster Comput.*, vol. 22, no. 5, pp. 11087–11099, 2019, [Online]. Available:

https://link.springer.com/article/10.1007/s10586-017-1304-7.

[40] C. Douligeris and A. Mitrokotsa, "DDoS attacks and defense mechanisms: classification and state-of-the-art," *Comput. Networks*, vol. 44, no. 5, pp. 643–666, Apr. 2004, doi: 10.1016/J.COMNET.2003.10.003.

[41] C. Arthur and J. Halliday, "Wikileaks under attack: the definitive timeline," *Guard.*, 2010, Accessed: May 03, 2020. [Online]. Available: https://www.theguardian.com/media/2010/dec/07/wikileaks-under-attack-definitive-timeline.

[42] BBC, "Anonymous hacktivists say Wikileaks war to Continue," *http://www.bbc.co.uk/news/technology-11935539*, 2010. https://www.bbc.com/news/technology-11935539 (accessed May 03, 2020).

[43] E. Protalinski, "Wikileaks has been under DDoS attack for the last five days | ZDNet," 2012. https://www.zdnet.com/article/wikileaks-has-been-under-ddos-attack-for-the-last-five-days/ (accessed Sep. 20, 2020).

[44] N. Wilcox, Z. Wilcox-o, D. Hopwood, and D. Bacon, "Report of Security Audit of Cryptocat," 2014.

[45] Open Technology Fund, "Third party audit of integrated SecureDrop Workstation completed - SecureDrop," 2019. https://securedrop.org/news/third-party-audit-integrated-securedrop-workstation-completed/ (accessed Sep. 09, 2020).

[46] S. Leible, S. Schlager, M. Schubotz, and B. Gipp, "A Review on Blockchain Technology and Blockchain Projects Fostering Open Science ," *Frontiers in Blockchain* , vol. 2. p. 16, 2019, [Online]. Available: https://www.frontiersin.org/article/10.3389/fbloc.2019.00016.

[47] L. W. Cong and Z. He, "Blockchain disruption and smart contracts," *Rev. Financ. Stud.*, vol. 32, no. 5, pp. 1754–1797, 2019.

[48] A. Saied, R. E. Overill, and T. Radzik, "Detection of known and unknown DDoS attacks using Artificial Neural Networks," *Neurocomputing*, vol. 172, pp. 385–393, Jan. 2016, doi: 10.1016/J.NEUCOM.2015.04.101.

[49] T. Liu *et al.*, "A New Bitcoin Address Association Method Using a Two-Level Learner Model," in *International Conference on Algorithms and Architectures for Parallel Processing*, 2019, pp. 349–364.

[50] S. Alam, "Testing the weak form of efficient market in cryptocurrency," *J. Eng. Appl. Sci.*, vol. 12, no. 9, pp. 2285–2288, 2017.

[51] Unstoppable Domains, "Unstoppable Domains," 2018. https://unstoppabledomains.com/ (accessed Mar. 21, 2020).

[52] Protocol Labs, "What is IPFS? – IPFS Documentation," 2017. https://docs.ipfs.io/introduction/overview/ (accessed Mar. 15, 2020).