Improved User Privacy in Social Networks Based on Hash Function

Kawthar Alrwuili[1] and Saloua Hendaoui[2]

1 kookdaily55@gmail.com 2 selhechi@ju.edu.sa

Department of computer Science, College of Computer and Information Sciences, Jouf University, Jouf, Skaka, Saudi Arabia

Abstract

In recent years, data privacy has become increasingly important. The goal of network cryptography is to protect data while it is being transmitted over the internet or a network. Social media and smartphone apps collect a lot of personal data which if exposed, might be damaging to privacy. As a result, sensitive data is exposed and data is shared without the data owner's consent. Personal Information is one of the concerns in data privacy. Protecting user data and sensitive information is the first step to keeping user data private. Many applications user data can be found on other websites. In this paper, we discuss the issue of privacy and suggest a mechanism for keeping user data hidden in other applications.

Key words:

Cryptography, encryption, privacy, security, social network, mitigation technique, hash, application, protection, web server, application server, database server

1. Introduction

With the development of technology and the invention of smartphones, which linked remote locations whenever and wherever communication and users' private data exchange became easier and faster. Social media networks are widely used and are exponentially developing. Several users nowadays are visiting social sites to communicate with their friends and relatives, share multimedia files, and even read news and novelties in different fields. It is one of the means that benefited from internet services, mobile technologies. Currently, various sectors and ministries benefited from the ease of sharing the content and raising educational issues of interest to the community for the public referendum. In addition, they can be used to achieve goals such as looking for work, spreading an idea, or opening a business.

There are a large number of social networking locales that there is no search engine for them. Further, there are particular sites that enable clients to make their social networking websites [1]. Sometimes, users are surrounded by ignorance and make many mistakes when using social networking services, for example, use of unapproved software, misuse of corporate computers, unauthorized access to physical and network, misuse of passwords, exchange of sensitive data between computers when working at home [2]. Wrong use brings risks, some viruses inject themselves into links in social networks, and while the user clicks on this link, this virus spreads in the device, and cybercriminals seek to draw the user's attention to the infected link or file, thus attracting them to click on it.

There are other ways to get your personal data, and that is by doing some online behavior without realizing that it puts you and your family's privacy at risk. An Example of a popular App, FaceApp is owned by the Russian company Wireless Lab, a program that predicts how your photo will be at an advanced age or look older, and in order to get the result and your future photo, the application must be granted permission to access and control images on the smartphone, and if this permission is necessary, this permission remains dangerous, Where you allow the application through this permission to access the camera, view device files, view networks, and others. It has sparked criticism for potential data misuse and privacy violations! [3]. Also other application, TikTok is owned by the Chinese Internet technology company "ByteDance" and was recently under investigation by UK authorities for potential mishandling of children's data [3].

2. Problems statements

2.1 Impact of social network on privacy

From stand-alone computers housing massive databases of governments and other large institutions to the current distributed computer networks with linked information, such as the World Wide Web, networked mobile devices, privacy has become an essential field in public discourse over these radical technological transformations [4]. The more information about individuals that is available online, the greater the risk of their privacy being stolen by people compiling their data and identifying their cross-cutting profile, such as location, online behavior, and interests, posing a threat to their safety and security [5]. Users' data may also be shared with third parties, leading to privacy breaches [6]. This gives people the ability to misuse this information maliciously to violate the privacy of the user.

Is not just about the user's behavior, a lot of breaches occur because of password breaches, it's one of the most common information security failures. The Central Intelligence Agency revealed in 2015 that 47 government

Manuscript received December 5, 2021
Manuscript revised December 20, 2021
https://doi.org/10.22937/IJCSNS.2022.22.1.15

institutions, including the Department of Homeland Security, had been hacked, allowing hackers access to over 21 million government employee accounts [7].

2.2 Mitigation used to enhance privacy

Because of privacy issues, user profiles must not distribute or circulate data throughout the internet, possible means to mitigate cyber security threats by building awareness regarding information disclosure by making customers aware of the disclosure of their personal information on sites, also by using more powerful anti-viruses with recent updates to achieve the proposed measures [1]. Many businesses are still struggling to keep passwords safe from hackers. According to a study given in [7], newly chosen strong passwords are related to a lower willingness to share personal information. The strength of a password was determined using methodology, which is based on information theory and predicts the number of guesses required. The strength of a password is calculated as a function of the implied character pool, which has 26 potential characters for each position if the password only contains lower case letters and 52 for each position if the password contains both lower and upper case letters. Similarly, if we add numbers, we will get a total of 10 potential characters. According to the study given in [8], the idea of deleting previous information was proposed because keeping old information would provide additional opportunities for attackers. As a result, determining the expiration time of the information, deleted or automatically encrypted at the time of expiration, provides additional privacy to eliminate old data and reduces threats.

These solutions are good for individual privacy but not enough; there are some problems we face in a lack of privacy. When searching the search index for someone's information does not precede personal knowledge, we will see some of his personal information, and some images published in that application because there is no privacy in those programs. The problem with security in social media applications is that they are developing protected programs and tools to make it an easy-to-use program. Some special applications for communication between the parties are protected by complete encryption developing their basic systems to encrypt messages during transmission and no unencrypted version is stored on service providers' servers [9]. For example, if we searched for someone we will find some of his personal information. The following Screenshot illustrates the lack of privacy in some applications.

Fig 1 Shows some information about someone name in different websites.

Moreover, when you click on one of these links, you will see some of his personal information. Here are some examples of well-known applications, and we have made the images blurry, respecting the privacy of the user:

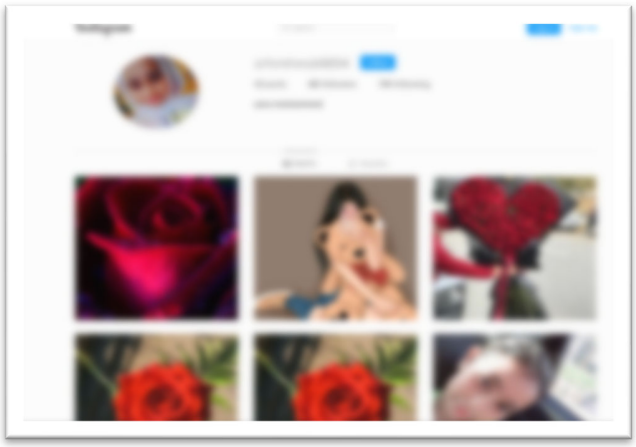

Fig 2.Information about Sara in Instagram application

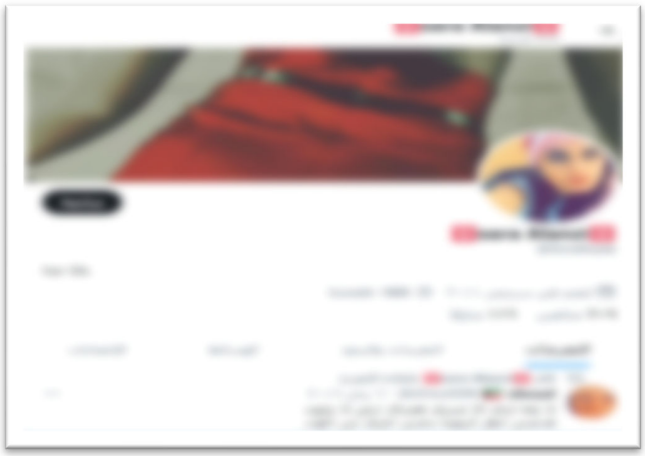

Fig 3.Information about Sara in Twitter application

While technological progress continues incessantly and contributes to the acquisition of information significantly, the importance of data confidentiality and user privacy must be considered. Therefore, one of the most essential sciences in the field of information technology is cryptography [10]. For example, the security of the email, password security, financial transaction security, and even electronic voting system security all require the same security objectives like confidentiality and integrity [11].

3. Cryptography

Cryptography is the practice of safeguarding data during transmission or storage by third-party adversaries, etymologically derived from the Greek words concealed and writing [10]. It achieves a number of security goals in order to protect data privacy [12]. In general there are three types of cryptography: Symmetric Key Cryptography, Asymmetric Key Cryptography and Hash Functions.

3.1 Symmetric Key Cryptography:

It is an encryption method in which the sender and receiver of a message encrypt and decode messages using a single common key [13, 14].

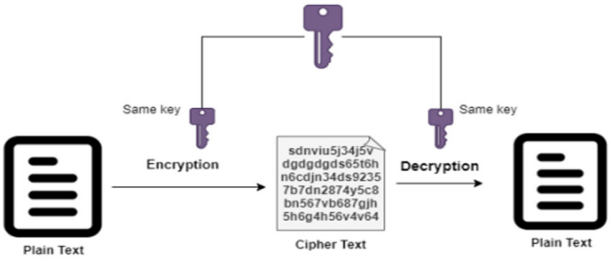

Fig 4. Symmetric Key Cryptography

3.2 Asymmetric Key Cryptography:

In this system, a public key is used for encryption and a private key is used for decryption; they are distinct from one another, and only the receiver can decrypt because he knows what the private key is [13, 15, 16].

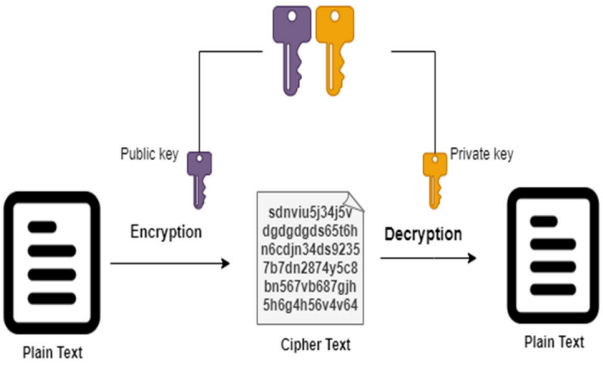

Fig 5. Asymmetric Key Cryptography

Each of these encryption methods has its own set of benefits and drawbacks; they are utilized in a variety of situations. Symmetric and asymmetric cryptographic systems will always be relevant to computer security as cryptography as a science evolves to protect against newer and more dangerous threats [17].

Several of algorithms in symmetric, including DES, 3DES, E-DES, AES, BLOW FISH, SEAL, RC2, RC4, and RC6; all are “bilateral” algorithms. In contrast, asymmetric algorithms, including RSA, ECC, EEE, DH, ELGAMAL ALGORITHM, and DSA, are relevant to “unilateral” algorithms [18].

Simar Preet Singh and Raman Maini [19] compared encryption algorithms and found that "Blowfish" performed better than other commonly used encryption techniques. AES performed poorly when compared to other algorithms, because it demands more processing resources.

Authors in [20] performed a comparison of DES, AES, RSA, and BLOWFISH algorithms, conducted with text files. The performance matrices are the Encryption time, Decryption time, and Throughput (results are summarized in table 1, 2 and 3)

Table 1: Comparison between various texts files Encryption algorithms

FILE	*AES (in msec)*	*DES (in msec)*	*RSA (in msec)*	*BLOWFISH (in msec)*
1 MB	80	136.2	425.6	133.2
2 MB	154.7	269.6	710.9	192.6
5 MB	376.1	665.4	1710.9	373.6
10 MB	683.7	1236.2	3017.1	702.5
20 MB	1350.5	2356.5	6641	1355.2

Table 2: Data table for Throughput of text files Encryption

FILE	*AES (in msec)*	*DES (in msec)*	*RSA (in msec)*	*BLOWFISH (in msec)*
1 MB	80	136.2	425.6	133.2
2 MB	154.7	269.6	710.9	192.6
5 MB	376.1	665.4	1710.9	373.6
10 MB	683.7	1236.2	3017.1	702.5
20 MB	1350.5	2356.5	6641	1355.2
Total	2645	4663.4	6528.6	2757.1
Throughput (KB/msec)	14.7	8.3	5.9	14.1

Table 3: Comparison between various texts files Decryption algorithms

FILE	*AES (in msec)*	*DES (in msec)*	*RSA (in msec)*	*BLOWFISH (in msec)*
1 MB	118.9	144.6	3.8	50.2
2 MB	197.6	269.6	3.5	126.3
5 MB	457.7	690.9	3.7	210.7
10 MB	897.5	1294.6	3.7	575.4
20 MB	1844.5	2744.2	4.0	1025.5

Table 4: Data table for Throughput of text files Decryption

FILE	*AES (in msec)*	*DES (in msec)*	*RSA (in msec)*	*BLOWFISH (in msec)*
1 MB	118.9	144.6	3.8	50.2
2 MB	197.6	269.6	3.5	126.3
5 MB	457.7	690.9	3.7	210.7
10 MB	897.5	1294.6	3.7	575.4
20 MB	1844.5	2744.2	4.0	1025.5
Total	3516.2	5143.9	18.7	1988.1
Throughput (KB/msec)	11.06	7.56	2080.85	19.57

According to results given in tables 1, 2 and 3, AES takes less time to encrypt text files while RSA takes less time to decrypt text files.
Also in another study [21] symmetric algorithms including DES, 3DES, AES, and BLOWFISH were implemented, and their performance was compared. The results showed that "Blowfish" had a very good performance. It was also discovered that AES outperforms 3DES and DES.

3.3 Hash Function Algorithm

This algorithm does not make use of any keys. A hash value with a fixed length is calculated based on the plain text, making it impossible to reconstruct the plain text's contents [13]. The significant distinction between hashing and other methods of encryption is that once data is encrypted, the process cannot be altered or read in any manner [13, 22]. The hashing algorithm determines the length of the output or hash. Hash lengths for the most popular hashing algorithms or functions typically range from 160 to 512 bits [23].

The most common hash functions used nowadays are dedicated hash functions, which are hash functions that are only utilized for hashing [24]. A cryptographic hash function compresses messages of any length into digests of a specific length [25]. It's a one-way operation that means it is impossible to compute the input from its output [22]. If you change one bit anywhere in the message, the entire hash value changes. This is called 'the avalanche effect' [23].
Some common hash algorithms are:

- MD5 (Message Digest 5)
  The outputs are a 128-bit length from an input of an arbitrary length message. MD5 is a renewal of MD4 [26].

- RIPEMD-160
  A well-known hash functions in the RIPEMD family. It generates a message digest that is 160 bits long. See (27, 24)
- Secure Hash Algorithm (SHA)
  The National Institute of Standards and Technology (NIST) publish a set of hash functions. All of the current SHA algorithms were developed by the NIST. All of the SHA algorithms were developed by the NIST: SHA-1, SHA-2, and SHA-3. NIST has made SHA 224, SHA 256, SHA 384, and SHA 512 as the new standard hash function. SHA-512 its predecessor is SHA1 [26].

Table 5: Differences in SHA algorithm Variation [26]

Algorithm	*Message Length (bit)*	*Block Size (in bit)*	*Word Size (in bit)*	*The Size of the Message Digest (bit)*
SHA 1	<264	512	32	160
SHA 256	<264	512	32	256
SHA 384	<2128	1024	64	384
SHA 512	<2128	1024	64	512

The conclusion performed in [28], that the running time of MD5 is faster than a SHA256 algorithm. Both have same complexity that is Θ (N).

3.3.1 HOW HASH FUNCTION WORKS?

Two methods are included: hashing by division and hashing by multiplication [29].

1- **Mod method:** map the key into one table slot by dividing the rest of the key by table size**.**
Hash table of size *m* and hash key *k*
Function; {hash (*k*) = *k* mod *m*}
For example: *K* = 43532, *m* = 20
The Result of the key of 43532 mod 20 is {12}**.**
Another hash Key = 5321 , 5321 mod 20 is {1}; notice we will get only number less than 20 because we are using MOD 20, so we have less than 20 different possible Hashing Values.
Notice if we have the Key = 4560 we get {0} nothing attached to 0 in the hash table.
Another hash key = 48741, 48741 mod 20 is {1}; Hence, it can be that many keys have the same hash value. This is called Collision.

(Sumagita, Meiliana, et al) in [26] perform comparison of multiple hash functions about collision, the table below show the comparison:

Table 6: Comparison of hash function about collision

Algorithm	*The size of the message digest (bit)*	*Message Block Size*	*Collision*
MD2	128	128	Yes
MD4	128	512	Almost
MD5	128	512	Yes
RIPEMD	128	512	Yes
RIPEMD128/256	128/256	512	No
RIPEMD160/320	160/320	512	No
SHA-0	160	512	Yes
SHA-1	160	512	There is a disability
SHA-256/224	256/224	512	No
SHA-512/384	512/384	1024	No
WHIRPOOL	512	512	No

2- **Multiplication method:** multiply the "*k*" by a constant real number c in the range 0 < c < 1 and extract the fractional part of *k* * *c*. Then, multiply this value by m and take the floor of the result.

Function: *{hash (k)* $= \lfloor (m * (k * c \bmod 1)) \rfloor$ *where* ***0 < c < 1****}*

For example**,** suppose that the word size of the machine is **w** bits and key fits into a single word, we restrict c to be fractional of the form s/2^{32}**:**
k= 123456, *p*= 14
M = 2^{14} = 16384, and *w* = 32
Then *k***s*= 327706022297664 = (76300*2^{32}) +17612864
So r1 = 76300 and r0 = 176122864. h(key) = 67

3.3.2 SHA General Steps [30]:

Step1: Padding the message
Step2: Parsing the padded message into 512-bits blocks
Step3: Initial hash value H (0)
Step4**:** Computing the final hash value H (N)
Step5**:** Generating the message digest by truncating H (N)

4. Methodology:

To provide privacy for users, we suggest encrypting users' data in applications servers thus information could not appear elsewhere. We suggest that these applications have a special file for their own Hash. After analyzing the literatures we focus on the SHA256 hash function. The owner of the application has a special file which is a table that has a user name with its hash value.

However, we have two assumptions; the first is that there is an agreement with the server that the application owners table keeps user names and their hash value to be private and not visible. The other assumption is to create a separate table to keep it aside. The Methodology is worked on the second assumption that the application's owner has a table separate from the server, and no one else can access it except the owner. The model below explains the idea of the proposed solution. Therefore, when the user comes and registers his data, this data will go to the application owner's database and encrypt the file and give it a value. The model below explains the idea of the proposed solution.

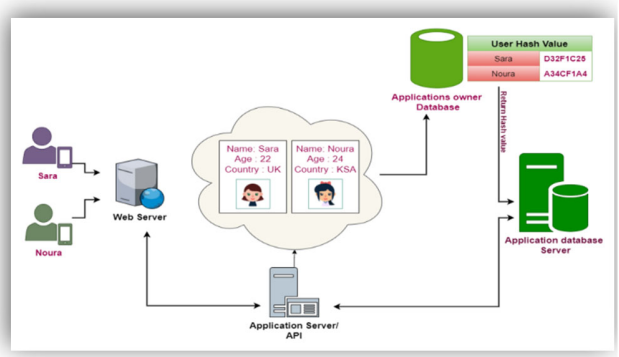

Fig 6. Methodology

4.1 Explaining the terms in the figure:

A web server is a computer program that runs continuously, waiting for users' requests coming over the internet. It consists of a sequence of web pages that allow the user to interact with the business logic. Web server uses the HTTP protocol to send webpages from websites to any client who requests them over the internet. Therefore, the Web server receives the request then returns results to the client if there are any. So, it is a client-server where the user interacts with the webserver via a browser. [31]

The application server works as a link between the web server and the application database. It's a program that receives and executes user requests. It's responsible for using network protocols to perform business logic. The distinction between an application and a web server is that an application server uses a set of protocols to perform business logic, whereas a web server processes HTTP requests and often delivers static content. [32, 33]

The database server provides the users data requested by the application server, which is efficient storage and transfer of data [34].

4.2 The Model Steps:

1- In client-server, a new user is coming to create an account and register his information by uploading a personal photo and other related special information.
2- Application server executes the user request and puts the user file in the owner's database as separate from the application database server.
3- The Owner's database executes the hash function in the file and returns a special hash value to application database server.

. Although, it can be said that it is possible to be know the hash value just by knowing the name of the person and anticipating several times until his information appears. So to make it more complicated, we add a username with the name and combine them and return the hash value. To make the approach clearer, for example, a person named Sarah registers her information (name, username, photo, etc.) the system takes the value of A (name) and B (username), combines them, and returns the hash value. Now, no one can decrypt the hash because no one knows the user's name except the user himself, because knowing the input data is the only way to decrypt a hash (see fig 7).

Hence, when we use a search engine to look up a user name after applying this approach, the information about the user who has registered in this application does not show.

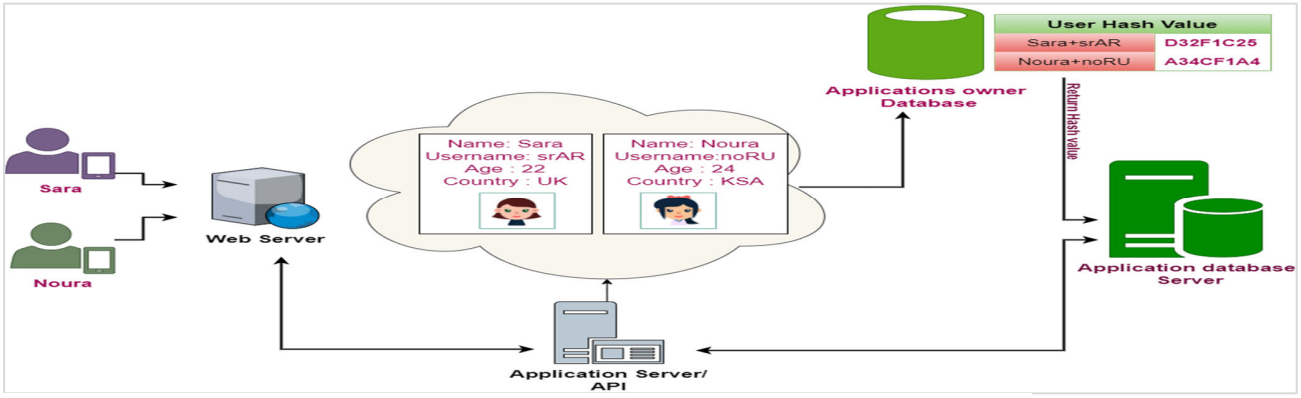

Fig 7. Proposed Methodology

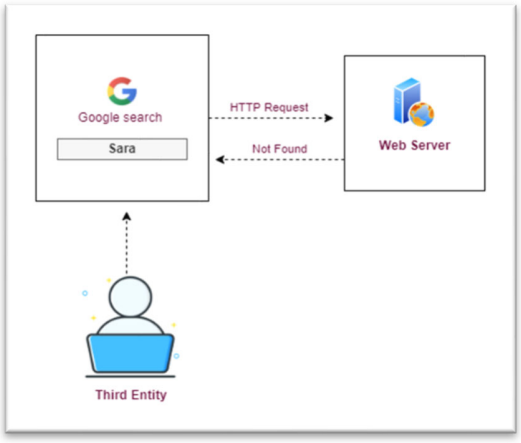

Fig 8.Search engine (Google)

5. Discussion

Cryptography is important to build security in today's world. The hash is considered more secure than symmetric and asymmetric; because it doesn't use a key for encryption or decryption. Also, the length of the output does not increase with the increase in the length of the input. It is used to digest the message. The one most commonly used and recommended by NIST is SHA-256 [35]. SHA-256 and SHA-512 are related, the point of properties of SHA-256 which differ from SHA-512 are: message size is 32 instead of 64 bits, steps of function is 64 instead of 80 iterations, and other properties [36]. Hash function is fast than other algorithms; however, it depends on the size of input. It is easy to compute, but it is impossible to invert the computation.

6. Conclusion and future work

Information is a very valuable commodity. It's crucial to understand who is watching our information and what they're doing with that data. In light of recent data leaks and violations, data security might be regarded as crucial factor for many consumers. In order To make data protected in social networks, we encrypt it. Hash functions play an important role in encryption, and what as we distinguished is that it is a one-way process and can only be decrypted by someone who knows the input.

Cryptography has then been able to use the properties of hash functions such as MAC, SHA, digital signature, password schemes, etc. Other properties are, collision resistance, and avalanche effect: this means that every small change in a message will change the major result in the hash value.

In this paper, we hope that we have explained the importance of hash functions in cryptography, and the difference between its algorithms. We suggested using the hash function to encrypt user information to provide security and privacy for sensitive information so that it is protected from intruders. The principle of security is that only authorized access can access sensitive information, which is the way you can demonstrate compliance with the security principle.

As a future work, we will study the complexity and cost of implementation of our proposal.

Acknowledgments

The authors would like to thank the Deanship of Graduate Studies at Jouf University for funding and supporting this research through the initiative of DGS, Graduate Students Research Support (GSR) at Jouf University, Saudi Arabia.

References

[1] Kumar, Sunil, and Vikash Somani. "Social media security risks, cyber threats and risks prevention and mitigation techniques." International Journal of Advance Research in Computer Science and Management 4.4 (2018): 125-129.
[2] www.securelist.com , «"Instant" threats », Denis Maslennikov, Boris Yampolskiy, 27.05.2008.
[3] BBC News (2019, July 18). FaceApp: Chuck Schumer asks for FBI investigation. Retrieved from https://www.bbc.com/news/world-us-canada-49027155
[4] Nissenbaum, H. Privacy as Contextual Integrity. Wash. L. Rev. 2004, 79, 101–139
[5] Shozi, N.A.; Mtsweni, J. Big data privacy in social media sites. In Proceedings of the 2017 IST-Africa Week Conference (IST-Africa), Windhoek, Namibia, Southern Africa, 30 May–2 June 2017; pp. 1–6
[6] S Ali ,N Islam ,A Rauf ,I.U Din ,and M Guizani ,and Joel J. P. C. Rodrigues. Privacy and Security Issues in Online Social Networks. 22 November 2018.
[7] Mamonov, Stanislav, and Raquel Benbunan-Fich. "The impact of information security threat awareness on privacy-protective behaviors." Computers in Human Behavior 83 (2018): 32-44.
[8] Lee, Phillip, et al. "Exploring privacy breaches and mitigation strategies of occupancy sensors in smart buildings." Proceedings of the 1st ACM International Workshop on Technology Enablers and Innovative Applications for Smart Cities and Communities. 2019.
[9] Botha, Johnny, W. C. Vant, and Louise Leenen. "A comparison of chat applications in terms of security and privacy." Proc. 18th Eur. Conf. Cyber Warfare Secur.. 2019.
[10] Mavroeidis, Vasileios, et al. "The impact of quantum computing on present cryptography." arXiv preprint arXiv:1804.00200 (2018).
[11] M. Campagna and C. Xing, "Quantum Safe Cryptography and Security: An Introduction, Benefits, Enablers and Challenges," ETSI, Tech. Rep. 8, 2015.

[12] Thambiraja, E., G. Ramesh, and Dr R. Umarani. "A survey on various most common encryption techniques." International journal of advanced research in computer science and software engineering 2.7 (2012).
[13] Dhivya, Mrs N., and Mrs S. Banupriya. "Network Security with Cryptography and Steganography." Int. J. Eng. Res. Technol 8.3 (2020): 1-4.
[14] Mouhib, Ibtihal. "Enhanced data security approach for cloud environment based on various encryption techniques." Journal of Theoretical and Applied Information Technology 80.3 (2015): 439.
[15] Guide, I.: Name the difference between symmetric and asymmetric cryptography. https://itinterviewguide.com/difference-between-symmetric-and-asymmetric/ (2016), (Accessed on 08/29/2018)
[16] Symmetric vs. Asymmetric Encryption – What are differences? https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences
[17] Гулієв, Нурал, and Віталій Волоховський. "SYMMETRIC AND ASYMMETRIC ENCRYPTION." Збірник наукових праць ΛΌГОΣ (2020): 88-90.
[18] Abood, Omar G., and Shawkat K. Guirguis. "A survey on cryptography algorithms." International Journal of Scientific and Research Publications 8.7 (2018): 495-516.
[19] Singh, Simar Preet, and Raman Maini. "Comparison of data encryption algorithms." International Journal of Computer Science and Communication 2.1 (2011): 125-127.
[20] Panda, Madhumita. "Performance analysis of encryption algorithms for security." 2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES). IEEE, 2016.
[21] Nadeem, Aamer, and M. Younus Javed. "A performance comparison of data encryption algorithms." 2005 international Conference on information and communication technologies. IEEE, 2005.
[22] Differences between Hash functions, Symmetric & Asymmetric Algorithms https://www.cryptomathic.com/news-events/blog/differences-between-hash-functions-symmetric-asymmetric-algorithms
[23] Examples of How Hashing Algorithms Work https://cheapsslsecurity.com/blog/decoded-examples-of-how-hashing-algorithms-work/
[24] Maetouq, Ali, et al. "Comparison of hash function algorithms against attacks: A review." International Journal of Advanced Computer Science and Applications, br 8 (2018).
[25] Andreeva, Elena, Bart Mennink, and Bart Preneel. "Open problems in hash function security." Designs, Codes and Cryptography 77.2 (2015): 611-631
[26] Sumagita, Meiliana, et al. "Analysis of secure hash algorithm (SHA) 512 for encryption process on web based application." International Journal of Cyber-Security and Digital Forensics (IJCSDF) 7.4 (2018): 373-381.
[27] F. Mendel, T. Peyrin, and M. Schl, ―Improved Cryptanalysis of Reduced RIPEMD-160,‖ Int. Conf. Theory Appl. Cryptol. Inf. Secuerty., pp. 484–503, 2013.
[28] Rachmawati, Dian, J. T. Tarigan, and A. B. C. Ginting. "A comparative study of Message Digest 5 (MD5) and SHA256 algorithm." *Journal of Physics: Conference Series*. Vol. 978. No. 1. IOP Publishing, 2018.
[29] What are Hash Functions and How to choose a good Hash Function? https://www.geeksforgeeks.org/what-are-hash-functions-and-how-to-choose-a-good-hash-function/
[30] Wu, Hongjun. "The hash function JH." Submission to NIST (round 3) 6 (2011).
[31] Yeager, Nancy J., and Robert E. McGrath. Web server technology. Morgan Kaufmann, 1996. Book
[32] What is a webserver and application server? https://hostman.com/blog/what-is-web-server/
[33] Oluwatosin, Haroon Shakirat. "Client-server model." IOSRJ Comput. Eng 16.1 (2014): 2278-8727.
[34] Bangare, S. L., et al. "Using Node. Js to build high speed and scalable backend database server." National Conference "NCPCI. Vol. 2016. 2016.
[35] Cooper, D., Apon, D., Dang, Q., Davidson, M., Dworkin, M., Miller, C.: Recommendation for stateful hash-based signature schemes. Technical report, National Institute of Standards and Technology (2019)
[36] Dobraunig, Christoph, Maria Eichlseder, and Florian Mendel. "Analysis of SHA-512/224 and SHA-512/256." International Conference on the Theory and Application of Cryptology and Information Security. Springer, Berlin, Heidelberg, 2015.

Kawthar Alrwuili: Master student in jouf university received the B.E.. degrees, from jouf University

Saloua Hendaoui received the B.E. and M.E. degrees, from Tunis Univ. in 2011 and 2009, respectively. She received the Dr.. degree from Cartage Univ. in 2017. Working as an assistant professor (from 2018) in the Dept. of computer Science Jouf University