HYBRIDIZED MODEL FOR DATA SECURITY BASED ON SECURITY HASH ANALYSIS (SHA 512) AND SALTING TECHNIQUES

Felix Aranuwa[1], Ford Olubodun[2] and David Akinwumi[1]

[1]Department of Computer Science, Adekunle Ajasin University,
Akungba – Akoko, Ondo State, Nigeria
[2]Department of Computer Science, Auchi Polytechnic, Auchi, Edo State, Nigeria

ABSTRACT

High-profile security breaches and attacks on many organization's database have been on the increase and the consequences of this, are the adverse effect on the organizations in terms of financial loss and reputation. Many of the security breaches has been ascribed to the vulnerability of the organization's networks, security policy and operations. Additionally, the emerging technology solutions like Internet-of-Things (IoT), Artificial Intelligence, and Cloud Computing, has extremely exposed many of the organizations to different forms of cyber-threats and attacks. Researchers and system designers have made attempts to proffer solution to some of these challenges. However, the efficacy of the techniques remains a great concern due to insufficient control mechanisms. For instance, many of the techniques are majorly based on a single mode encryption techniques which are not too robust to withstand the threats and attacks on organization's database. To proffer solution to these challenges, the current research designed and integrated a hybridized data security model based on Secured Hash Analysis (SHA 512) and Salting Techniques to enhance the adeptness of the existing techniques. The Hash Analysis algorithm was used to map the data considered to a bit string of a fixed length and salt was added to the password strings essentially to hide its real hash value. The idea of adding salt to the end of the password is basically to complicate the password cracking process. The hybridized model was implemented in Windows environment using python 3.7 IDE platform and tested on a dedicated Local Area Network (LAN) that was exposed to threats from both internal and external sources. The results from the test show that the model performed well in terms of efficiency and robustness to attacks. The performance of the new model recorded a high level of improvement over the existing techniques with a recital of 97.6%.

KEYWORDS

LAN, Threats and Attacks, Security Breaches, Cryptography, Data Security, Hash Analysis, Salting Techniques.

1. INTRODUCTION

Today, our society and the world at large have come to depend majorly on computers, information systems and technology for our day-to-day activities and business operations. This coupled with the rapid development of the internet and the rise of e-business, data exchange and communication over the network. According to [1], this development have resulted to a number of high-profile security breaches and attacks such as unauthorized access, online bullying, hacking, data disruption, data theft, modifications and so on. The devastating impacts of these attacks on any business include data loss, employee downtime and cost of restoring operations. To individual and organizations, it often results in reputation damage, financial loss and Loss of business opportunities [2].

DOI: 10.5121/ijnsa.2022.14203

In 2018, the study of Ponemon Institute on cost of data breach revealed that on an average, the damage caused by a data breach in the USA alone was $7.91 million. About 31,465 user accounts were impacted in the average data incident, which means beyond financial loses, most incidents leads to loss of customer trust and damage to reputation [3]. According to [4], during the pandemic, and besides the ensuing economic effects, companies around the globe embattled with increased rates of cyber-attacks. Unfortunately, African countries seem to be a major targets. In the year 2020, the survey of Sophos Group, a British security software and hardware company, revealed that 86% of Nigerian companies fell prey to cyber-attacks within the past year. This happened to be the second highest percentage recorded globally after India and much higher than that of South Africa with 64%. This survey made use of data from 65 Nigerian companies that host data on public cloud-based services like Azure, Oracle, Amazon Web Services (AWS), Alibaba cloud, and others. This means that, about 56 out of 65 companies fell prey to various forms of cyber-attacks such as malware, ransomware, and data leaks during the period considered. According to the report, Nigeria had the highest percentage of data leakages worldwide, and ranks in the top five for other forms of attacks such as cryptojacking. The percentage breakdown of cyber-attacks on Nigerian companies and global cloud security incidents are depicted in Figure 1 and Figure 2 respectively.

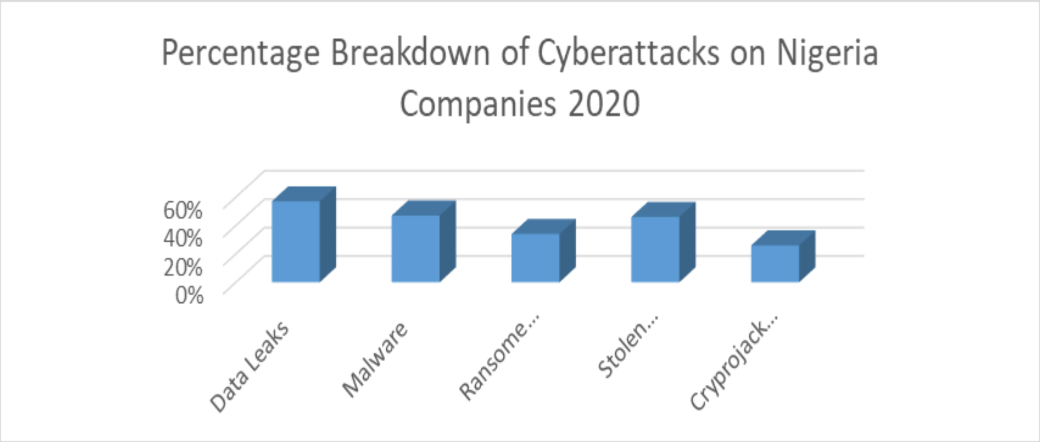


Figure 1. Percentage of Breakdowns of Cyber-attacks on Nigeria Company 2020 :Source: [5]

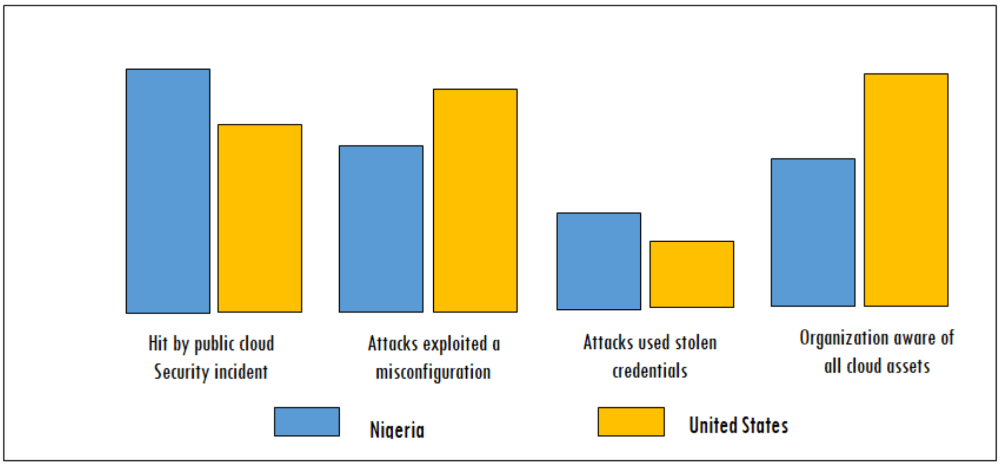


Figure 2. Global cloud security incidents: Source: [5]

Generally, information systems are vulnerable to technical, organizational, and environmental threats. Figure 3 depicts samples of these threats to each component of a typical network.

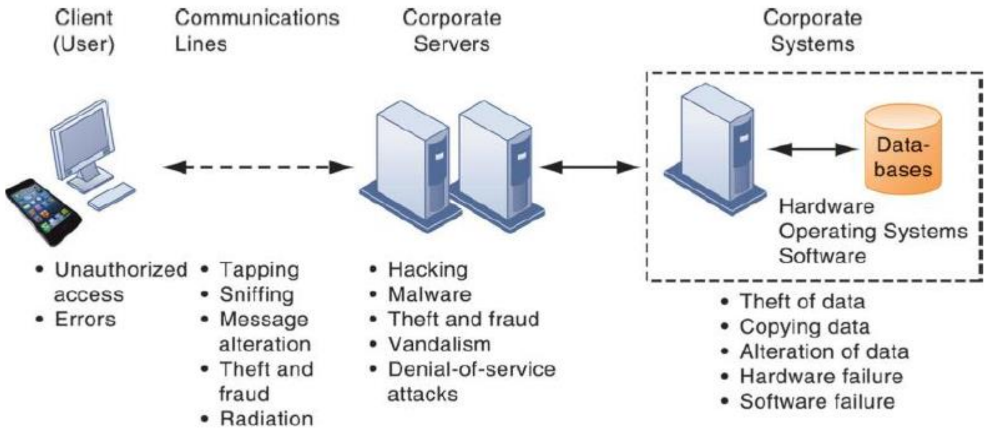


Figure 3. Example of threats to each component of a typical network: Source: [6]

According to [7], presented in Figure 4 are some of the likelihood threat vectors that occurs in a workplace.

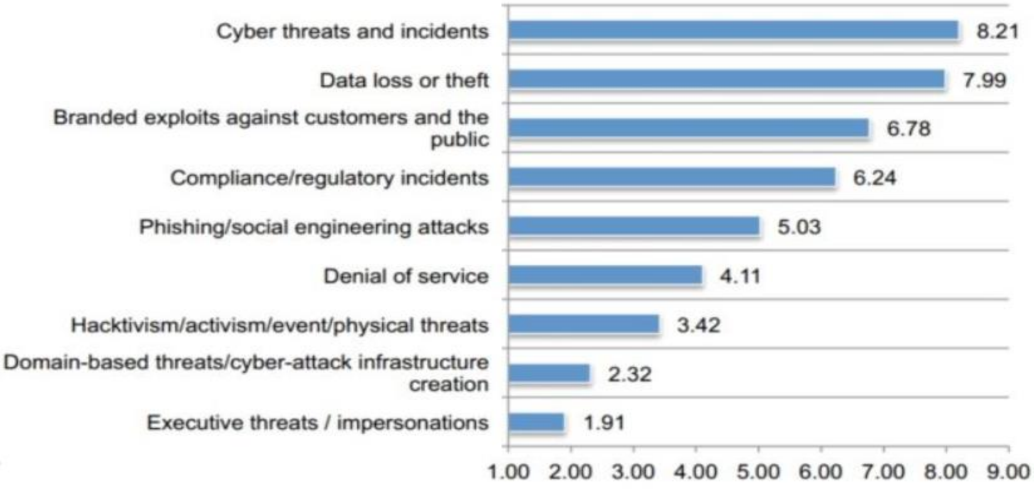


Figure 4. Likelihood threat vector occurring in a workplace :Source: [8]

In the light of the above, organizations and database administrators are expected to ensure proper protection of their operation and sensitive data. To achieve this, a definite and consistent security policies are expected to be followed, coupled with deployment of numbers of mechanism in order to create different layers of security around their database. According to [9], the mechanisms may vary from security features of authentication, encryption and firewalls that could secure the network against hackers

2. LITERATURE REVIEW

2.1. Overview of Data Security

Data security has been described as the practice of protecting digital information from unauthorized access, corruption, or theft throughout its entire lifecycle. The process includes data encryption, data backups, intrusion detention and prevention, identity and access management, hashing, tokenization, and other key management practices that can protect data across all applications and platforms [10];[11].

According to [11], data security is a concept that encompasses every aspect of information security from the physical security of hardware and storage devices to administrative and access controls, as well as the logical security of software applications, organizational policies and procedures. This suffices to say that, protecting sensitive information requires far more than implementing basic security technologies such as an antivirus solution and a firewall. Today, security of data involves a wide and complex set of protective measures against both accidental and intentional unauthorized access and modification that can lead to data corruption or loss. Meanwhile, one major key to data and information security is access control [3].

According to [6], access control to a system or network provides a way of granting or restricting privileges to users or groups on organization database objects. However, studies and incidences have shown that malicious users can infer sensitive information or circumvent insufficient and or weak control mechanisms. Some of the works reviewed are [12; 13; 14; 15; 16; 17; 18; 19; 20]. Many of the techniques are majorly based on a single mode encryption techniques which are not robust enough to withstand the threats and attacks. Meanwhile, data encryption can provide a very strong security for data at rest. However, encrypted data can be hacked or decrypted with time and computing resources. Studies also revealed that hackers prefer to steal encryption keys or intercept data before encryption or after decryption. Additionally, the most common way to hack encrypted data is to add an encryption layer using an attacker's key [21]. To proffer solution to the above challenges, a hybridized model for enhanced data security using Security Hash Analysis (SHA 512) and Salting Techniques to improve the efficiency of the existing mechanisms is presented in this work.

2.2. Hashing Analysis and Salting Techniques

Adding Salt to Hashing is a better practice to store passwords and secure sensitive data. A salt added to hashing process enforces their uniqueness, increase their complexity without increasing user requirements to mitigate attacks [22].

2.2.1. Hashing Analysis

According to [22], hashing is the practice of using an algorithm to map data of any size to a bit string of a fixed size length. Hash algorithm is a strong password storage strategy that is critical to mitigating data breaches that may put the reputation of any organization in danger. Its value is sometimes called hash code or hash sums. In cryptography, a hash function is a mathematical algorithm that maps data of any size to a bit string of a fixed size. The function input can be refer to as message or simply as input. The fixed-size string function output is known as the hash or the message digest. The hash functions used in cryptography have the following key properties:

(i). Practically, it is easy to compute, but difficult or impossible to re-generate the original input, unless the hash value is known.

(ii). It is difficult to create an initial input that would match a specific desired output.

Thus, in contrast to encryption with two way mechanism, hashing is a one-way mechanism. This implies that the data that is hashed cannot be practically "unhashed".

Mathematically, a typical hash function H that accepts a variable length block of data M as input can produce a fixed size hash value $h = H(M)$. With modular hashing, the hash function is simply $h(k) = k \bmod m$ for some m (usually, the number of buckets). The value k is an integer hash code generated from the key. If m is a power of two (i.e., $m=2p$), then $h(k)$ is just the p lowest-order bits of k. Figure 5 shows a typical hashing process.

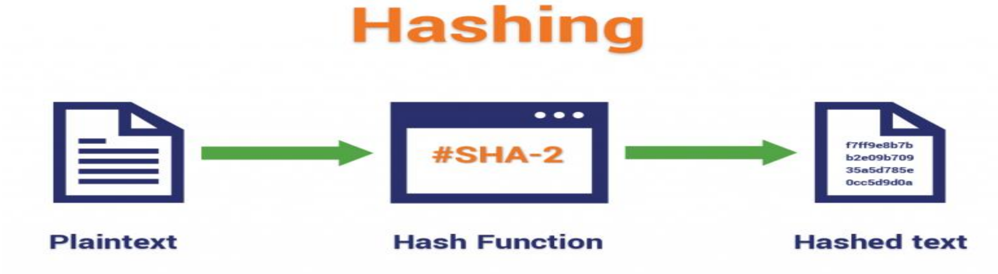


Figure 5. Typical Hashing Process : Source: [23]

Common Hashing Algorithms include: MD4, a self-loathing hash algorithm, **MD5** is another hashing algorithm made by Ray Rivest that is known to suffer vulnerabilities. Another type is Security Hashing Algorithm (SHA), which is best known as the hashing algorithm used in most Secure Sockets Layer/Transport Layer Security (SSL/TLS) cipher suites. A cipher suite is a collection of ciphers and algorithms that are used for SSL/TLS connections. SHA handles the hashing aspects. The SHA has different versions such as SHA-1, now deprecated. Other type is SHA-2, sometimes known as SHA-256. Other variants with longer bit lengths are also available such as RIPEMD, a family of cryptographic hashing algorithms with a lengths of 128, 160, 256 and 320 bits. It was developed under the framework of the EU's Project Ripe by Hans Dobbertin and a group of academics in 1996. Its 256 and 320 bit variants do not actually add any additional security, but diminish the potential for a collision. WHIRLPOOL is another type of hashing algorithm, it produces 512-bit hashes that are typically represented as 128-digit hexadecimal numbers. The TIGER, is a fairly new algorithm that is beginning to gain some attractions with file sharing networks and torrent sites [22].

2.2.2. Salting Techniques Algorithm

According to Open Web Application Security Project (OWASP) guidelines, a salt is a value generated by a cryptographically secure function that is added to the input of hash functions to create unique hashes for every input**.** The idea of adding a salt to the end of a password is essentially to complicate the password cracking process. By salting your password you are essentially hiding its real hash value by adding an additional bit of data. Figure 6 depicts the interaction process of salt and hash algorithms. According to [23], salting is a concept that is typically pertains to password hashing. Essentially, it is a unique value that can be added to the end of the password to create a different hash value. This adds a layer of security to the hashing process, specifically against brute force attacks. A brute force attack is where a computer or botnet attempt every possible combination of letters and numbers until the password is found. Common salting algorithms with specific features that help to boost security include Argon2, scrypt, bcrypt and PBKDF2, [24].

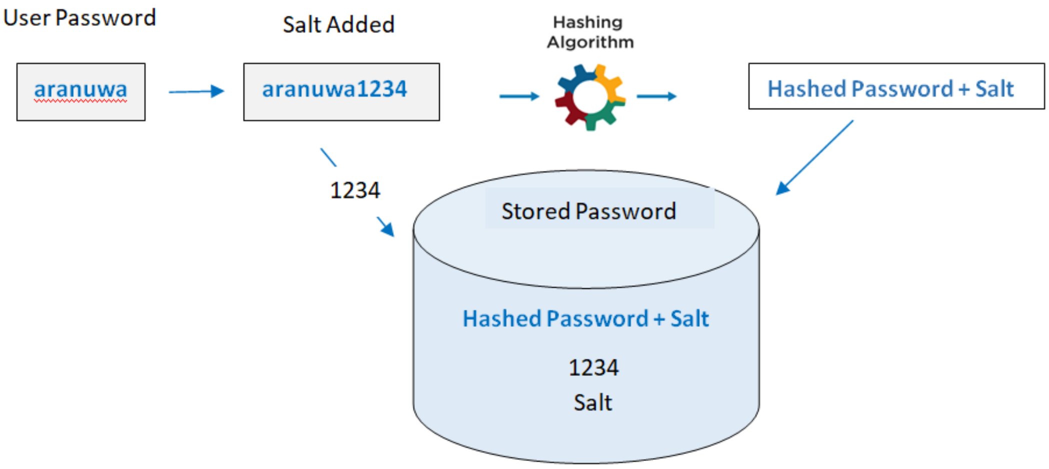


Figure 6. Salt and Hash Algorithms Process

3. METHOD AND MATERIALS

To achieve the objective of this work, the researchers first reviewed some literatures in the domain to know what has been done, and thereafter designed a hybridized data security model based on Secured Hash Analysis (SHA 512) and Salting techniques to enhance the adeptness of the existing techniques.

3.1. The Architecture of the Hybridized Data Security Model

The conceptual diagram of the data security model is presented in Figure 7. The hybrid data security system combines the salt and hash algorithms.

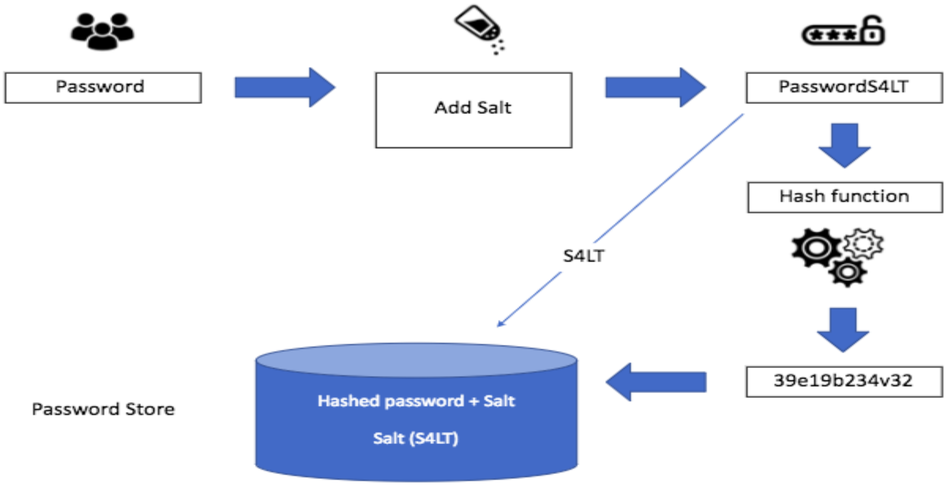


Figure 7. Conceptual diagram of the Hybridized Data Security Model

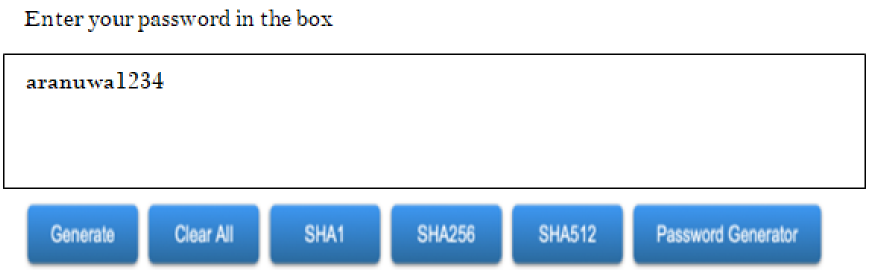
The process involve adding the salt to the initial password and the new password string is generated, which is fed into the hashing system to produce a newly hashed result. The hashing component involves the process of storing the passwords and authorization in form of digital data of a fixed length in the database as shown in Figure 7. SHA 512 algorithm was used in the hashing process component. A typical hash algorithm is stated as follows:

```
Generate (x and y)
Exchange x and y
If $x=y=m_g$, then
Get n; $P = H_1$; $Q = H_1$;
Else if $(x-y=n_g)$ then
get n $P = H_2$; $Q= H_2$;
else if $x=y=ug)$ then
get n; $P =H_3$; $Q = H_3$;
else if $(x=y=s_g)$ then
get n; $P = H_4$; $Q = H_4$
else default
end if
end
```

where,

m_g: *greater no of lower case Alphabetic*
n_g: *greater no. of Numeric character*
u_g : *greater no. of Upper case Alphabetic*
s_g: *greater no. of special character*

The model was implemented in Windows environment using python 3.7 IDE platform. The model was tested on a dedicated Local Area Network (LAN), which was exposed to threats from both internal and external sources with good upshot. Figure 8 depict how a typical password could be generated.

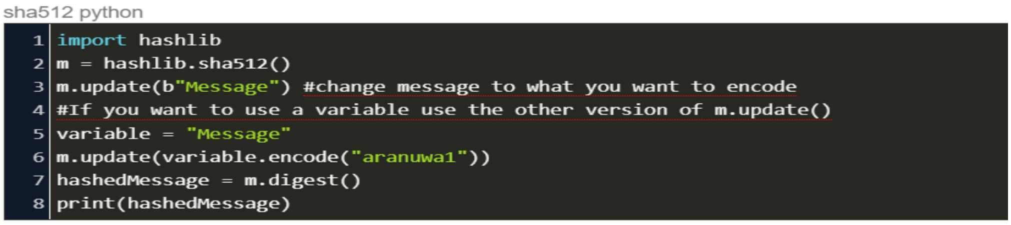


Enter your password in the box

aranuwa1234

Figure 8. Password Generator

Figure 9 depict sample codes of how the hash value was calculated in python programming.



sha512 python

```python
import hashlib
m = hashlib.sha512()
m.update(b"Message") #change message to what you want to encode
#If you want to use a variable use the other version of m.update()
variable = "Message"
m.update(variable.encode("aranuwa1"))
hashedMessage = m.digest()
print(hashedMessage)
```

Figure 9. Hash calculation using python code

4. CONCLUSION AND RECOMMENDATION

The quest for an efficient data security mechanism that will proffer solutions to the high-profile security breaches and attacks on many organization's database motivated this research. Studies and incidences showed that the emerging technology solutions like Internet-of-Things (IoT), cloud computing and the high rate of business data communication on the internet has awfully exposed many organizations to different forms of cyber-attacks. The consequence of this digital warfare on many organization include data loss, financial loss and damage of reputation. Hence, this work presented an efficient data security model that can tackle the present challenges of data breaches and improve on the existing techniques. The model integrated Secured Hash Analysis (SHA 512) and Salting techniques to enhance the adeptness of the existing techniques. The results from the experiment show that the model performed well in terms of robustness to attack and efficiency. The performance of the new model when compared with existing techniques showed a recital of 97.6%. The model is therefore recommended to database administrators and business organizations for adequate security on their databases and transaction processes.

REFERENCES

[1] Hubschmid, F (2021). How To Protect Your Small Business From Cyber Threats. Retrieved on 11/02/2022 at https://www.forbes.com/sites/theyec/2021/06/02/how-to-protect-your-small-business-from-cyber-threats/?sh=408e0fae56cd

[2] Taylor, T (2020). How Reputational Damage from a Data Breach Affects Consumer Perception. *Security Links*. Retrieved on 22/2/2022 at https://www.securelink.com/blog/reputation-risks-how-cyberattacks-affect-consumer-perception/.

[3] Brooks, R (2019). Data Security Explained: Definition, *Concerns and Technologies. Security and Compliance, Netwrix Blog. Retrieved on 11/2/2022.*

[4] Emmanuel, P (2020). Nigerian companies record 2nd highest percentage of global cyber-attacks. *Techpoint, Africa*. Retrieved on 11/02/22 at https://techpoint.africa/2020/07/17/nigerian-companies-global-cyberattacks/.

[5] Sophos Group (2021). The state of cloud security 2020. *Sophos Group Limited*. Retrieved on 11/02/2022 from https://secure2.sophos.com/en-us/content/state-of-cloud-security

[6] Laudon K. and Laudon, J (2017). Management Information Systems (15th Ed), Pearson, 2017.

[7] Larry, B (2016). 10 Common IT Security Risks in the Workplace. *Contemporary Computer Services International (CCSI).* https://www.ccsinet.com/blog/page/6/

[8] Ponemon Institute (2018). Security beyond the Traditional Perimeter; Retrieved on 22/2/2022 at https://www.ponemon.org/, https://cdn2.hubspot.net/hubfs/30658/Ponemon_External_Threat_2016__ExecSumm.pdf

[9] Georgiana, M and Marius, V (2013). A Hybrid Approach of System Security for Small and Medium Enterprises; combining different Cryptography Techniques. *Proceeding of the 2013 Federated Conference on Computer Science and Information Systems* . 1(1), 659-662.

[10] Microfocus (2020). What is Data Security? *Microfocus Limited*. Retrieved on 14/11/2021 at https://www.microfocus.com/en-us/what-is/data-security.

[11] IBM (2021). Why is data security important? Retrieved on 11/02/2022, at *https://www.ibm.com/topics/data-security#:~:text=Data%20security%20is%20the%20practice,theft%20throughout%20its%20entire%20lifecycle.*

[12] Ajayi O.O and Falana T.J (2017). Empirical Evaluation of Data Hashing Algorithm for password checks in PHP webapps using salt and pepper. *Computing, Information Systems, Development Informatics & Allied Research Journal*. 8(1), 21-28. Available online at www.cisdijournal.net.

[13] Mohammed, A.M.A and Prakash, K. (2014). Hybrid combination of message encryption techniques on Arabic text using new symmetric key and simple logarithm function. *International Journal of Science Knowledge Computing and Information Technology 2(1), 35-41.*

[14] Prerna, M. and Abhishek, S. (2013). A Study of Encryption Algorithms AES, DES and RSA for Security. *Global Journal of Computer Science and Technology Network, Web & Security* 12(15), 34-46.

[15] Kakkar, A, Singh M. L. and Bansal P.K (2012). Comparison of various Encryption Algorithms and Techniques for Secured Data Communication in Multimode Network, *International Journal of Engineering and Technology*, 2(1), 87-92.

[16] Pavithra S and Ramadevi E. (2012). "Performance Evaluation of Symmetric Algorithms, *Journal of Global Research in Computer Science*, 3(8), 43-45.

[17] Obulam, S. Mani, U, Nanaji, Y. and Swapna, S (2012). A New Method in Symmetric Encryption for Block Cipher Module: A Bit Shifting approach. *IJAIR*, ISSN: 2278-7844.

[18] Tat-Wi, C. (2010). "Implementation of Hybrid Encryption Method using Caesar Cipher Algorithm" Unpublished Master Thesis, University Malaysia Pahang (UMP). Pahang Malaysia.

[19] Ramaraj, E., Karthikeyan, S. and Hemalatha, M. (2009). A design of security protocol using hybrid encryption technique. *Inter. Journal of the Computer, the Internet and Management*, 17(1), 78-86.

[20] Shaar, M., Saeb, M., Elmessiery,M and Badawi, U (2003). A Hybrid Hiding Encryption Algorithm (HHEA) for Data Communication Security. *Proceedings of 2003 IEEE 46th Midwest Symposium on Circuits and Systems*, Cairo, Egypt. pp. 476-478.

[21] Chu, M (2022). Can Your Encrypted Data Be Hacked? *University of North Georgia*. Retrieved 0n 11/2/2022 from https://dataoverhaulers.com/can-encrypted-data-be-hacked/

[22] Arias, D (2019): Hashing Passwords: One-Way Road to Security. *Auth0 Inc*. Retrieved on 11/2/2022 from https://auth0.com/blog/authors/dan-arias/

[23] Nohe, P (2018). The difference between Encryption, Hashing and Salting. Retrieved on 11/2/2022 from https://www.thesslstore.com/blog/difference-encryption-hashing-salting/#:~:text=Hashing%20is%20the%20practice%20of,is%20a%20one%2Dway%20function.

[24] Lake, J (2018). Encryption, hashing, salting – what's the difference?. *Comparitech Limited.*UK. Retrieved 14/02/2022 from https://www.comparitech.com/blog/information-security/encryption-hashing-salting/