Sensitive Data Exposure: Data Forwarding and Storage on Cloud Environment

https://doi.org/10.3991/ijoe.v17i14.27365

Shahad Alotaibi[1](✉), Khadijah Alharbi[1,2], Balsam Abaalkhail[2], Dina M. Ibrahim[1,2]
[1]Qassim University, Buraydah, Saudi Arabia
[2]Tanta University, Tanta, Egypt
421200274@qu.edu.sa

Abstract—Sensitive data has become an essential part of life today. With the increase in sensitive data, the importance of maintaining its confidentiality and integrity has increased. One of the solutions became to store this data in the cloud. But the risk of revealing this data still exists. This is because the rate of attack, leakage and loss of this data has become a serious matter. The importance of sensitive data in our current era is considered our oil, as it is very important in several uses in statistical analyzes and other important matters that help the authorities to know the type of people and their interests, and when publishing this information it is important to know what information should be available and What information should not appear or be used on the sites. In this paper, discuss this issue, which is one of the most important security issues that is sensitive data exposure. We touched on this research and the techniques used to reduce these risks to the data stored in the cloud. Mention the types of sensitive data and the types of attacks that may affect these data, and mention the points of weakness, and then the methods of protecting this data.

Keywords—sensitive data exposure, cloud computing, information, detection

1 Introduction

Disclosure of sensitive data in storage, transmission, and permanent use in many locations poses a major risk to users' privacy. With the technical development that we live in the last five years from 2015 to 2021, It has published Statista magazine, Statistics about the number of Internet users in the world, and is Statistical review by Joseph Johnson published the date Jan 27, 2021, "How many people use the internet?

Almost 4.66 billion people were active internet users as of October 2020, encompassing 59 percent of the global population. Mobile has now become the most important channel for internet access worldwide as mobile internet users account for 91 percent of total internet users [1].

We know now that the use of the Internet and websites has become an essential part in various aspects, this is why the increase in Internet users on websites or surfing the

Internet requires new methods of data protection, especially sensitive data. Sensitive data can be any information that is needed to be secured from unauthorized access. Sensitive data can be banking information, Social Security numbers, and login credentials.

Many papers discuss preserving information and ways to protect it. One of the proposed solutions is to preserve the information and avoid its exposure to danger or disclosure, as they suggested storing the information in remote places such as the cloud and storing it in areas that are difficult to obtain, but the protection of information via the cloud is still a matter under study, as it is also vulnerable to attackers. Insiders and outsiders.

The rest of this paper is organized as follows; Section II, literature review, in this section, issues related to sensitive data are discussed. Section III, discussion, in the discussion section, we touched on sensitive data and its types, what are the methods used to attack this sensitive data, and the extent of the danger and spread of data in the environment of the cloud, and access to this data has become easier. Section IV. Data protection techniques concludes this paper discussing the possible methods and types of data protection. And to raise awareness, and reduce the risks in attacking this type of data in the framework of the cloud.

2 Literature review

In this section, we review some studies that measure the impact of sensitive data on the Internet world or the technology world in particular. We talked about some technologies that helped protect information, but the issue of protecting sensitive data needs to be further developed in the use of the presented technologies.

Obaida, M. et al. [2] they presented the Secure Sensitive Data (SSD) Eclipse Integrated development environment plug in. This tool will help bridge the gap for sensitive data theft. Also, it provides real time interactive security feedback to Java developers. The SSD uses static analysis of Java Applications for detecting security vulnerabilities. In order to keep sensitive data encrypted and managed right in the web application, the authors focus on five rules. Given that rules, by presenting icons and messages that describe the bugs with the written code and feedback on how to resolve them, the tool can alert the user. Then they analyzed the tool on three separate metrics: coverage of recommendations, enhancement of programmers, and overhead of the tool.

Muhasin, H. et al. of [3] focused on factors that effect on the decision of management information systems on sensitive data in public cloud like: Data Confidentiality, Availability, Privacy, Integrity, Authentication, Anonymity, Authorization and Defining the responsibilities. Also conduct Interviews and surveys to explain the impact of these factors on the decision in managing information systems on sensitive data in cloud environments.

Shu, X. [4] A system has been proposed to detect the leakage of sensitive data to preserve confidential information and the ability to control sensitive information and not to disclose it or make use of it in a misplaced legal position. A mysterious fingerprint system has been proposed that helps enhance the privacy of data during the detection of data leakage from private files and E-mails. It helps and enables the data owner to delegate the task of securely examining the content to the inspection service providers without disclosing sensitive data to preserve its privacy, and that is by getting to know the DLD provider and Internet service provider (ISP) provider to cooperate between them in preserving the data without spreading it.

Bentajer, A. et al. of [5] they proposed Cloud system CS-IBE, a scheme based on Identity-Based Encryption (IBE) through Library Pairing Based Cryptography (PBC). The system is designed to secure confidentiality of data against unauthorized, harmful and unauthorized access. The proposed design allows cloud users to securely process and store their data. It also assures that IBE's flexible and expandable key management without an increasing key store is secure. They introduced the design implementation and verified it by an empirical analysis.

El Makkaoui [6] This research aims to develop the speed of verifying the security of the information in the data stored in the cloud because most of those who use the cloud use devices with limited resources such as (mobile phones, tablets, and etc.) The researchers' proposal was to use homomorphic encryption (HE) so that the third party could have the ability to deal with confidential data and information, and Cloud-Paillier scheme has also been proposed, which will help in the decryption process faster while maintaining the level of security in the data and the level of encryption. The effectiveness of the Cloud-Paillier scheme has been proven through experimental simulation work. About the effectiveness of decoding speed and maintaining the level of security.

Table 1 explains how quickly the suggested scheme responds to the decoding and verification of data, while maintaining the level of information security.

Table 1. Decryption time performance [6]

Plaintext Bit Size	Cloud-Paillier	Cloud-Paillier's Variant
100	2189.96 ms	252.33 ms
200	2052.52 ms	243.80 ms
300	2175.62 ms	251.96 ms
400	2180.17 ms	250.29 ms
500	2109.57 ms	247.35 ms
600	2036.49 ms	241.33 ms
700	2015.63 ms	240.28 ms
800	2042.99 ms	245.39 ms
900	2034.51 ms	238.47 ms
1000	2181.36 ms	253.25 ms

Sulochana, M et al. of [7] they provided an efficient model for data security and integrity stored using the multi cloud method. Solving the challenges of data security in the public environment. Multi cloud strategy uses two or more distinct cloud to reduce the risk of failure of service availability, data loss, and privacy loss. The system introduced provides a stable and secure infrastructure that facilitates user data protection and defends the system from other external agents. To ensure data security, the data is encrypted by using the RSA encryption algorithm. They present how the system operates and evaluate the results provided by the system.

Similarly, authors in [8] proposed a system that stores EHR in the cloud, using a blockchain known as MediBchain platform, also using PAU Private Accessible Unit as a Trusted Third Party (TTP) of a system which is a medium between user and blockchain. The system is divided into two levels, first contains Registration Unit information and second contains blockchain. Sensitive patient's data are stored in the blockchain to obtain security and integrity and other part of the EHR data is stored in the cloud in encrypted format using ECC.

Sastry, K. et al. of [9] proposed a system to prevent access patterns of personal and business data with Novel approach by profiling user behavior to confirm if and when a malicious insider criminally accesses someone sensitive data in the cloud services. Also use decoy technology that allows them to keep decoy information or dummy information in the file system to deceive insider data theft attackers.

In [10], this paper is based on the security of personal information in the internet sales to study security of data privacy. The personal information divided into general information and critical information to ensure it does not leak out of the private data and stored by private cloud. Also adopt the membership degree to define the selection of trust cloud. And then compare experimental results and results of selected trust cloud with Qos evaluation.

Authors in research [11], the researchers explored the attacks facing the data that are dealt with in the cloud and that is stored in many cloud resources. The researchers looked at the most important sources that must be dealt with in complete confidentiality and to have adequate protection steps implemented, which is the hypervisor because it is the first source of data access and transfer of resources. It has also been hoped that attacks targeting the side channel in the cloud will be detected. Examples of these technologies are RSA and AES. It has also been suggested in this research about attacks that target the cloud and the success rate of these attacks.

The research needs an additional survey about the most important protection methods in the infrastructure of the cloud and the structure of the resources through which this data is transferred.

Kholidy, H. et al. of [12] they presented an approach to detect Impersonation attacks in Clouds. Three different mechanisms are proposed to detect Impersonation attacks. The first method was to evaluate a series of associated system calls from the operating systems of VMs. The second evaluates the Network Flow data from the network environment. Third, by using neural networks to produce better detection. Through two intrusion detection frameworks, CIDS and CIDS-VIRT (Cloud Intrusion Detection Dataset) they evaluated the models.

Researchers in [13] propose the Proficient Security over Distributed Storage (PSDS) method, which aims to protect data in cloud computing. It has been recognized in recent years that the increasing use of cloud computing in uploading and preserving data reduces the burden on storage space of the resources used. This research suggested the PSDS system in protecting information by dividing the information is divided into two parts. A part that carries public information and a part that carries sensitive information.

The sensitive information is divided into two other parts and divided into two types of clouds. After that, the encryption key is applied to the sensitive information, and then they are combined and combined with the public information, and then the decryption key is applied to obtain on a general text. This research is compared with other research focused on technologies such as SA-EDS, Reliable Framework for Data Administration (RFDA), Encryption and Splitting Technique (EST) to secure data storage over multi-cloud.

Table 2. Comparison of techniques in protecting data in the cloud

Technologies	Purpose	Research
data-leak detection (DLD)	**Detected data:** This technology aims to maintain the privacy of data leak detection as it helps the data owner in the data authorization process without revealing sensitive data, and it also adds to Internet service providers to offer their customers DLD technology as an additional service with strong privacy guarantees.	Shu, X. et al. of [4]
(IBE) Identity-Based Encryption	Proposed Cloud System CS-IBE to secure confidentiality of data against unauthorized, harmful and unauthorized access. Also allows cloud users to securely process and store their data.	Bentajer, A. et al. of [5]
Multi cloud strategy. RSA encryption algorithm.	provided an efficient model for data security and integrity stored in the public environment using the multi cloud method	Sulochana, M et al. of [7]
MediBchain blockchain ECC encryption for data in cloud.	Proposed system that stores EHR in cloud, using MediBchain blockchain where sensitive patient's data stored in the blockchain to obtain security and integrity and other part of the EHR data is stored in the cloud in encrypted format using ECC.	Alomar et al. of [8]
Novel approach decoy technology	Prevent access patterns of personal and business data with Novel approach by profiling user behavior to confirm if and when a malicious insider criminally accesses someone sensitive data in the cloud services Also use of decoy technology to deceive insider data theft attackers.	Sastry, K. et al. of [9]
CIDS and CIDS-VIRT (Cloud Intrusion Detection Datase)	Presented an approach to detect Impersonation attacks in Clouds	Kholidy, H. et al. of [12]
Proficient Security over Distributed Storage (PSDS) method	**Protected data:** This technology aims to protect data as it is able to add protection to data as it divides the data into two parts, part general data and sensitive data, and this technology divides sensitive data into two parts, and each part is encrypted and distributed on a multiple cloud, and public data is encrypted and uploaded to One cloud. **Detected data:** This technology has also been tested against multiple attacks, and the results show that it is resistant to the main attack associated with cipher text and plain text attacks.	Shahid, F et al. of [13]

According to Table 2, some studies have suggested effective systems or solutions by using different technologies to protect the confidentiality and security of sensitive data in either a public or private cloud environment. Where some technologies depend on data encryption algorithms. It also protects data against threats and attacks targeting sensitive data.

On the other hand, some research has provided solutions for detecting and preventing attacks such as impersonation attacks and detecting data leaks.

3 Sensitive data discussion’s

In this section will discuss all the problems of sensitive data that have been addressed by many types of research in the revolution of technology development and the increase in data around us and the extent of the impact of this data on the surroundings of personal life and work, we will discuss methods of protection and ways to maintain the level of data security in technologies The modernity, and because the cloud is considered the modern technology in the field of data preservation as a third party and to reduce the burden of data on devices. At the end of the research, will discuss the data problems in the cloud and the techniques used to protect data in the cloud.

3.1 Overview of sensitive data

When sensitive data exposure may occur? If a company or any entity inadvertently exposes personal data. Also, it is a result of not protecting a database adequately in storing their information. This may be a result of weak encryption. Another, if someone mistakenly uploads information to an incorrect database [14].

3.2 Sensitive data types

Different kinds of data may be exposed in a sensitive data exposure. Credit card numbers, Banking account numbers, Social Security numbers, healthcare data, home address, phone numbers, dates of birth, session tokens, and user account information such as usernames and passwords are some kinds of data that can be left exposed.

3.3 Sensitive data attacks

Component many types of attacks can expose sensitive data. These include:

SQL injection attacks. It is the most common application attack. 65 percent of the time, this occurs when bad users manipulate SQL queries to perform malicious commands. Sometimes these commands are intended to reveal sensitive data. Figure 1 shows how SQL Injection can occur, by entering a malicious parameter that appears as a normal input or request but is actually malicious. On the other hand, servers must provide protection against these attacks, otherwise this data becomes vulnerable [15].

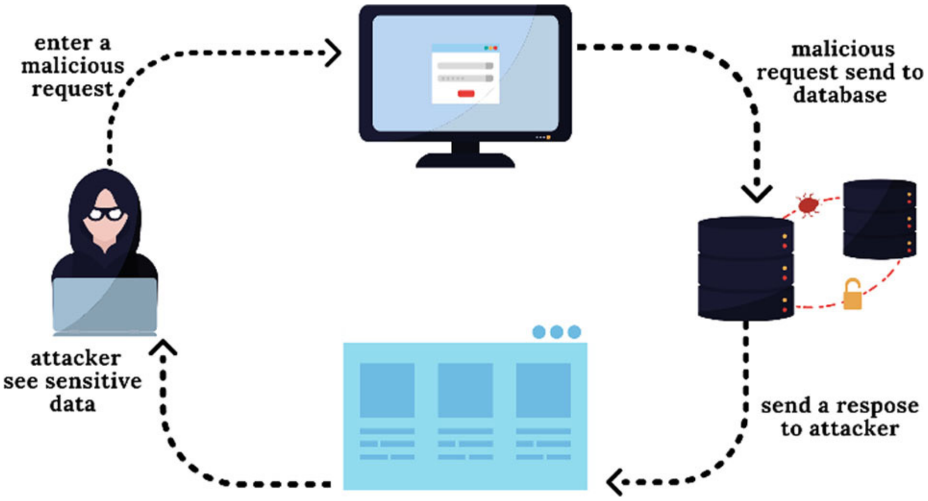
enter a malicious request
malicious request send to database
attacker see sensitive data
send a respose to attacker

Fig. 1. SQL injection example

Phishing attacks. This type often occurs in emails or text messages with the aim of capturing sensitive data from the user without knowing him. Where the attacker deceives the victim by directing him to a site that appears as a confiscated site. The victim enters his sensitive data and the attacker steals it [16].

Insider threat attacks. This is the kind of risk that many companies face. It is a danger to the employees. As they can see some sensitive data. It is possible that some of them steal it or exploit it in an illegal way [17].

Ransomware attacks. It is one of the malicious programs that may affect the victim's device through a link that the victim thinks is a reliable link. But once you click on this link, this malicious program is downloaded, and then the attacker can see the victim's sensitive and confidential data to seize this data and harm the victim [18].

3.4 Vulnerabilities and problems facing data protection

We know that data protection plays an important role in organizations and employees are the main driving factor in methods of preserving and protecting information, and it is important to develop the working staff around information protection due to the complete control and access of employees to the resources of devices and the Internet completely [19].

Hackers can exploit this control and access to find vulnerabilities or send vulnerabilities to the network, and they are used without the employees' knowledge of their dangerousness.

And among the risks that have been addressed in many types of research on information breach in many organizations and institutions are [19]:

1. Entering illegal sites without the knowledge
2. The use of personal company accounts in public sites
3. Leave sensitive data open for a while on the sites

4. Data theft
5. Use of unsafe (open) networks

With the increase in the use of the Internet and the conversion of all services into electronic services, whether for the public sector, the private sector, or individual uses, many companies, and government agencies have been exposed to security breaches due to the lack of experience of employees about the most important risks that may cause information breach and the most important methods that may lead to the disclosure of this information [19].

3.5 Data breaches in cloud computing

Data breaches are a security event in which sensitive data is copied and used in illegal projects, and this data is used by plundering and exploiting by an unauthorized person, and sensitive data may be personal information, trade secrets, intellectual information, personal inventions, and Other information that revolves around the same person only, without the intervention of a third party, and these data may be related in several fields such as education, industry, health information, financial services, and others[20].

It is important to develop information security in those agencies that contain information on a large number of people, which may cause a disaster in the event of a security failure in their system, so there must be many security precautions [20–24].

One of the most famous problems facing sensitive information that targets people without knowing what is happening around them is social engineering social engineering is one of the most important threat factors in cybersecurity, which may put organizations and individuals at risk, Figure 2. Shows the method of social engineering and how to benefit from it in several ways [11].

Because of the nature of humans to trust people without knowing their insides, caution must be taken and there are limits in the disclosure of personal information, and it is important to ensure the use of strong accounts and confidential numbers that are difficult to violate and not to link these numbers to personal things [11].

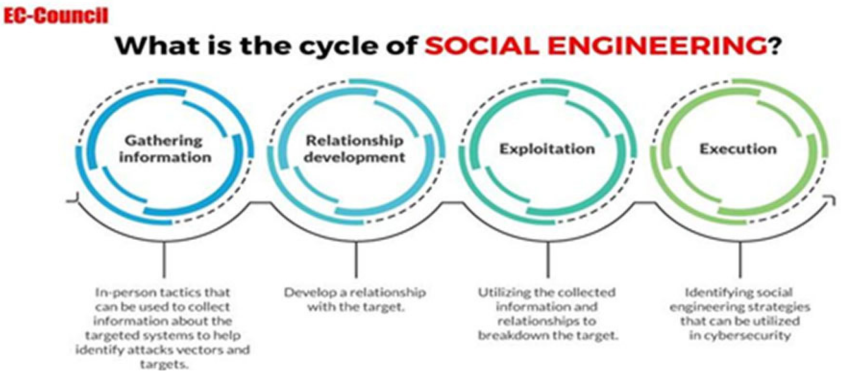
EC-Council
What is the cycle of SOCIAL ENGINEERING?
Gathering information
Relationship development
Exploitation
Execution
In-person tactics that can be used to collect information about the targeted systems to help identify attacks vectors and targets.
Develop a relationship with the target.
Utilizing the collected information and relationships to breakdown the target.
Identifying social engineering strategies that can be utilized in cybersecurity

Fig. 2. Life cycle of social engineering

Five Ways to Protect Yourself [11]:

1. Avoid E-mail that contain a request for personal information, such as requesting the year of birth, graduation date, and other personal information that helps the attacker guess the passwords of your accounts.
2. Social engineers may deceive the victim by asking for help or providing a specific service in exchange for a specific offer, as they cheat on many aspects of assistance in exchange for simple information that may be used in illegal exhibits.
3. One of the most famous types of hacks in which social engineers scam is spam, as it is a source for them to provide accounts and fake sites with you in exchange for obtaining correct personal information through this mail, it is necessary to cancel advertising subscriptions to the E-mail and avoid opening random E-mail.
4. Be sure to provide protection programs on your laptop or mobile device, as they help reduce attacks and preserve sensitive information. Be sure to update the system, as it is one of the most important reasons that help devices maintain a normal level of security, and use VPN connection.
5. Knowledge and reconnaissance is the best proof in knowing the types of possible attack and the forms of attack that are aimed at obtaining sensitive information for the victim. It is necessary to know in the field of cybersecurity and to follow up on organizations supporting this field, as it is our current age.

Recommendations are to enter training courses in the field of cybersecurity and knowing the dangers of this field, and many organizations in Saudi Arabia offer training courses of excellent and enriching quality such as the Ministry of Communications and information technology, the Saudi Federation for Cybersecurity [11].

Take care not to divulge the national identity number, as it is the primary target for an attacker of sensitive information.

And other information such as full name, phone number, marital status, and bank accounts.

4 Data protection techniques

Until transferring client data to the cloud, using a variety of methods to secure it. The research group has proposed a variety of masking strategies related to the variety of data security situations. While this variety can be perplexing, it also has the benefit of allowing for the management of a wide range of privacy and accessibility requirements [25]. This session will focus on some of the more recent data protection techniques that have been used or may be used to allow privacy in the cloud.

4.1 Data splitting techniques

Data splitting is a security procedure that uses fragmentation-sensitive data and stores the fragments in specific form in separate areas. Fragments should be designed in such a way that a single fragment does not cause the subject to be re-identified, nor does it disclose sensitive information that can be attached to a particular subject [18].

Data splitting workflow. Data can be outsourced to multiple cloud accounts within the same CSP or to different clouds, each operated by a different CSP running much of the same service, by a local proxy executing data separating, for example a multi-cloud [18].

The workflow for data segmentation and storage is illustrated in the Figure 3. The proxy first collects the data to be outsourced from the customer and evaluates the possibility of exposure. To use it, the proxy uses the user's privacy specifications (Step 0 in Figure 3.), which determine the collection of attributes that may lead to re-identification. The proxy then determines how data is separated and also how many storage locations are required to avoid disclosure; each data fragment is a collection of data that can be securely stored together. Also, it keeps the splitting criteria and storing positions in a local database (Step 2). Finally, each data fragment is forwarded to a different CSP (Steps 31 to 3n).

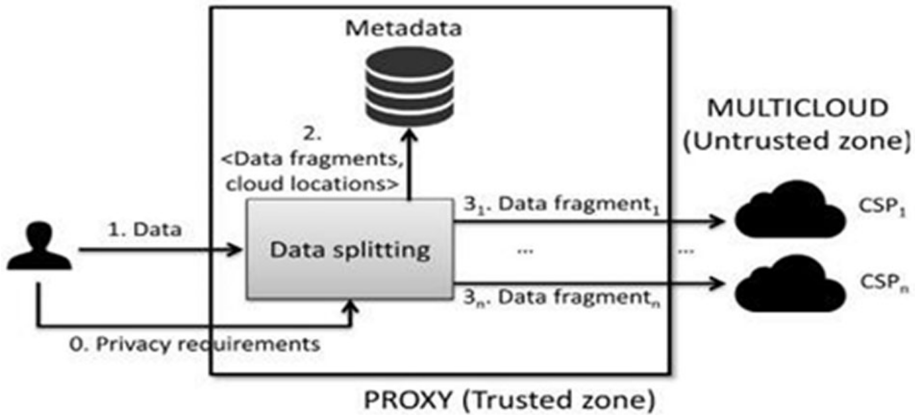

Fig. 3. Data storage and splitting workflow in a multi-cloud environment

4.2 Data anonymization methods

Data anonymity helps to maintain the confidentiality of data and maintain the privacy of data, and it is done by dividing the data (and also encrypting the data).

Disseminating data and making them open source may be exploited as a third party in unreliable science, the exposed data may be handled in a useful way in the analysis process and beneficially make use of it, but it must be that this data does not directly affect people or link it. Of specific individuals and this may enter into the personal information of individuals [25].

Encrypted data may be useless for people who do not know about encrypting this data, other than data that may be anonymous, but which has a benefit for all uses.

Cloud computing offers high areas of information storage, and cloud providers may provide services in dealing and analyzing data, service providers may provide data encryption services and anonymous data analysis services, and the main advantage in dealing with anonymous data and encrypted data is the speed of dealing with anonymous data, it is easier and faster in the process of analysis and ease of processing. The use of anonymity is done by storing the data in the cloud [26–28].

Attributes can be classified as

A. Identifiers. The identifiers contain sensitive personal information and may be exposed and tampered with, and this information may be such as (Social Security Number). These features must be removed from anonymous groups and replaced with random values.

B. Quasii-dentifiers. It is the scattered information that is not known directly. There must be causes or complementary information to it to arrive at an explicit identifier, such as the information may contain age and standard of living, and through this information, the extent of the person's knowledge may be reached. The semi-identifiable information is anonymous.

C. Confidentiality. It is the sensitive features and characteristics of the individual, and it may be information that pertains to the individual and does not belong to personal identity information. External information can be used without changing the basic information or entering it, and it is considered useful orders for the analytical benefit.

D. Non confidential attributes. Non-confidential features are which general and inaccurate information can be used. They are considered open data and are subject to publication and public use and do not require any influences or consequences that may hinder their personal.

E. Non-perturbative. There is an inference from public information to private information by deriving this information, pivoting it and making use of it in a second way, and making it a source in the analysis.

There is exploitation in data analysis by showing some data as general data, but it carries meanings and personal details and sensitive data, and some data is attributed to different people. However, troubled masking may preserve the statistical properties of the original data better than non-per durative masking. The best-known perturbative masking methods are

Privacy models: The data privacy system requires the addition of many resources to maintain the level of privacy of the data, and the type of data must be preserved. It may require very sensitive data, publishable data, and data that must be in the privacy field only. Analysis of some data requires that the data be public and it is not private, but it may be that this data after analysis brings sensitive and accurate data, by adhering to the privacy model, it is necessary to take into account the type of privacy, the type of data level, and the external data from the public cloud, regardless of the type and size of the cloud.

4.3 Cryptographic techniques

Most of the other technology plans deployed to resolve privacy issues in the cloud include cryptography as one of the strongest and most significant building blocks. Modern cryptography has grown to serve a wide range of real-world security requirements, many of which are relevant to cloud computing. Cryptography as a field reflects a large variety of information security goals, user architectures, and functionalities [24, 29].

Because of the recent data leak outbreak, many cloud storage providers now use cryptographic solutions to encrypt the data they hold, especially symmetric encryption techniques like AES-256. However, Since the CSP also handles all of keying content in such services, the protection of the data security is ultimately dependent on the consumers' interest in the CSP [25,30].

There are many mechanisms that enable clients to send an encrypted data set to the cloud while also allowing the cloud to execute useful functions on the data set such as:

A. Public-key encryption. The receiver produces two keys: a public key that can be shared with the public and a private key that is kept a secret. The security properties of PKE schemes ensure that if the sender knows the public key, he or she will produce cipher texts that are intended to be transmitted to the recipient.

B. Identity-based encryption. Depending on a central point of authority they are used at the same time by a group of people, each of whom is given a unique identity by the central authority. Strings, such as a name or an e-mail address, are used to describe identities in this context.

C. Searchable encryption. Previous to outsourcing, secure the data by encrypting it in a way that makes for highly secure search.

D. Order-preserving encryption. Enable for the encryption of numerical data in a manner that allows the encrypted data to be compared, and hence the cipher texts to be ordered according to their corresponding plaintext values. For one-dimensional set queries, as well as maximum, minimum, and top queries, OPE schemes are a very effective solution.

5 Conclusion

Security of sensitive data has become an important matter with the development of technology and its remarkable progress, and all transactions are made via the internet, and the information must carry correct values to be dealt with in government agencies and official agencies in the provision of electronic services. Information is stored through the cloud, and it is necessary to raise the level of security in the cloud to preserve the sensitive and private information of people, such as personal photos, identity numbers, and other sensitive personal data. Information should be secure in the cloud. In the future, we seek to discuss and develop one of the techniques that help provide adequate protection in the cloud and preserve sensitive information specifically that is stored in the cloud.

6 References

[1] Imran, K., Anjum, N., Alghamdi, A., Shaikh, A., Hamdi, M., and Mahfooz, S. (2022). A Secure and Efficient Cluster-Based Authentication Scheme for Internet of Things (IoTs). Computers, Materials & Continua, 70(1), 1033–1052. https://doi.org/10.32604/cmc.2022.018589

[2] Obaida, M. A., Nelson, E., Ee, R. V., Jahan, I., and Sajal, S. Z. Interactive sensitive data exposure detection through static analysis. In 2017 IEEE International Conference on Electro Information Technology (EIT) May, 2017, IEEE, pp. 270–275. https://doi.org/10.1109/EIT.2017.8053368

[3] Muhasin, H. J., Atan, R., Jabar, M. A., and Abdullah, S. (2018). The factors affecting On Managing Sensitive Data in Cloud Computing. Indonesian Journal of Electrical Engineering and Computer Science, 1: 01–02. https://doi.org/10.11591/ijeecs.v11.i3.pp1168-1175

[4] Junaid, M., Shaikh, A., Hassan, M. U., Alghamdi, A., Rajab, K., Reshan, A., and Alkinani, M. (2021). Smart Agriculture Cloud Using AI Based Techniques. Energies, 14(16), 5129. https://doi.org/10.3390/en14165129

[5] Bentajer, A., Hedabou, M., Abouelmehdi, K., and Elfezazi, S. (2018). CS-IBE: a data confidentiality system in public cloud storage system. Procedia Computer Science, 141: 559–564. https://doi.org/10.1016/j.procs.2018.10.126

[6] El Makkaoui, K., Ezzati, A., Beni-Hssane, A., and Ouhmad, S. (2018). A swift Cloud-Paillier scheme to protect sensitive data confidentiality in cloud computing. Procedia computer science, 134: 83–90. https://doi.org/10.1016/j.procs.2018.07.147

[7] Sulochana, M., and Dubey, O. (2015). Preserving data confidentiality using multi-cloud architecture. Procedia Computer Science, 50: 357–362. https://doi.org/10.1016/j.procs.2015.04.035

[8] Al Omar, A., Bhuiyan, M. Z. A., Basu, A., Kiyomoto, S., and Rahman, M. S. (2019). Privacy-friendly platform for healthcare data in cloud based on blockchain environment. Future generation computer systems, 95: 511–521. https://doi.org/10.1016/j.future.2018.12.044

[9] Sastry, K. N., Rao, B. T., and Gunasekhar, T. (2015). Novel Approach for Control Data Theft Attack in Cloud Computing. International Journal of Electrical and Computer Engineering (2088-8708), 5: 1545–1552. https://doi.org/10.11591/ijece.v5i6.pp1545-1552

[10] Qiong, S., Liu, M., and Pang, S. (2013). Cloud computing application of personal information's security in network sales-channels'. TELKOMNIKA Indonesian Journal of Electrical Engineering, 11: 7331–7338. https://doi.org/10.11591/telkomnika.v11i12.3619

[11] Narayana, K. E., and Jayashree, K. (2020). Survey on cross virtual machine side channel attack detection and properties of cloud computing as sustainable material. Materials Today: Proceedings, 45: 6465–6470. https://doi.org/10.1016/j.matpr.2020.11.283

[12] Kholidy, H. A. (2021). Detecting impersonation attacks in cloud computing environments using a centric user profiling approach. Future Generation Computer Systems, 117: 299–320. https://doi.org/10.1016/j.future.2020.12.009

[13] Shahid, F., Ashraf, H., Ghani, A., Ghayyur, S. A. K., Shamshirband, S., and Salwana, E. (2020). PSDS–Proficient Security Over Distributed Storage: A Method for Data Transmission in Cloud. IEEE Access, 8: 118285–118298. https://doi.org/10.1109/ACCESS.2020.3004433

[14] Shaikh, A., Uddin, M., Elmagzoub, M. A., and Alghamdi, A. (2020). PEMC: Power Efficiency Measurement Calculator to Compute Power Efficiency and CO_2 Emissions in Cloud Data Centers. IEEE Access, 8, 195216–195228. https://doi.org/10.1109/ACCESS.2020.3033791

[15] Shar, L. K., and Tan, H. B. K. (2012). Defeating SQL injection. Computer, 46: 69–77. https://doi.org/10.1109/MC.2012.283

[16] Alsharnouby, M., Alaca, F., and Chiasson, S. (2015). Why phishing still works: User strategies for combating phishing attacks. International Journal of Human-Computer Studies, 82: 69–82. https://doi.org/10.1016/j.ijhcs.2015.05.005

[17] Zhu, D., Jung, J., Song, D., Kohno, T., and Wetherall, D. (2011). TaintEraser: Protecting sensitive data leaks using application-level taint tracking. ACM SIGOPS Operating Systems Review, 45: 142–154. https://doi.org/10.1145/1945023.1945039

[18] Mohurle, S., and Patil, M. (2017). A brief study of wannacry threat: Ransomware attack 2017. International Journal of Advanced Research in Computer Science, 8: 1938–1940.

[19] Tayan, O. (2017). Concepts and tools for protecting sensitive data in the IT industry: a review of trends, challenges and mechanisms for data-protection. International Journal of Advanced Computer Science and Applications, 8: 46–52. https://doi.org/10.14569/IJACSA.2017.080207

[20] Aljumah, A., and Ahanger, T. A. (2020). Cyber security threats, challenges and defense mechanisms in cloud computing. IET Communications, 14: 1185–1191. https://doi.org/10.1049/iet-com.2019.0040

[21] Mohammad Tabrez Quasim, et al., 5v's of big data via cloud computing: uses and importance, Sci.int(Lahore), vol.31(3), 367–371, 2019.

[22] Dr. Md. Tabrez Quasim and Mohammad. Meraj, Big Data Security and Privacy: A Short Review, International Journal of Mechanical Engineering and Technology, 8(4), 2017, 408–412. http://www.iaeme.com/IJMET/issues.asp?JType=IJMET&VType=8&IType=4

[23] M.T. Quasim, Security Issues in Distributed Database System Model , COMPUSOFT, An international journal of advanced computer technology, 2 (12), December-2013 (Volume-II, Issue-XII).

[24] M.T. Quasim, An Efficient approach for concurrency control in distributed database system, Indian Streams Research Journal, 2013(Volume-3, Issue-9).

[25] Naveed, Q. N., Qureshi, M. R. N. M., Shaikh, A., Alsayed, A. O., Sanober, S., and Mohiuddin, K. (2019). Evaluating and ranking cloud-based e-learning critical success factors (CSFs) using combinatorial approach. IEEE Access, 7, 157145–157157. https://doi.org/10.1109/ACCESS.2019.2949044

[26] Li, N., Qardaji, W. H., and Su, D. (2011). Provably private data anonymization: Or, k-anonymity meets differential privacy. CoRR, abs/1101.2604, 49: 55–60.

[27] Soobia, S., Asadullah, S., Syed, M. R. N., and Muhammad, A. M. (2018). Impact Of Data Mining Techniques To Analyze Healthcare Data. In Journal of Medical Imaging and Health Informatics, Vol. 8 (5), 674–682. https://doi.org/10.1166/jmihi.2018.2385

[28] Al Tayeb, A., Alghatani, K., El-Seoud, S., and El-Sofany, H. (2013). The impact of cloud computing technologies in e-learning. International Journal of Emerging Technologies in Learning (iJET), 8(2013). https://doi.org/10.3991/ijet.v8iS1.2344

[29] El-Seoud, S. A., El-Sofany, H. F., Abdelfattah, M., and Mohamed, R. (2017). Big Data and Cloud Computing: Trends and Challenges. International Journal of Interactive Mobile Technologies, 11(2). https://doi.org/10.3991/ijim.v11i2.6561

[30] Chen, M., and Lin, Y. (2019). Exploration and Implementation of Intelligent Park Information System based on Cloud Computing and Internet of Things. International Journal of Online & Biomedical Engineering, 15(1). https://doi.org/10.3991/ijoe.v15i01.9783

7 Authors

Shahad Alotaibi is an IT graduated student in college of computer, Majmaah University, Majmaah, Saudi Arabia. Student Cybersecurity in college of computer, Qassim university, Buraydah, Saudi Arabia. (E-mail: 421200274@qu.edu.sa)

Khadijah Bandar Alharbi is a Computer Science graduate student in College of computer & information technology, Tabuk University, Tabuk, Saudi Arabia. Student Cybersecurity in college of computer, Qassim university, Buraydah, Saudi Arabia. (E-mail: 421214478@qu.edu.sa)

Balsam Abaalkhail is an IT graduated student in College of Computer, Qassim university, Buraydah, Saudi Arabia. Student Cybersecurity in college of computer, Qassim university, Buraydah, Saudi Arabia. (E-mail: 421200473@qu.edu.sa).

Dina M. Ibrahim is an assistant professor at the department of Information Technology, College of Computer, Qassim University, Buraydah, Saudi Arabia from September 2015 till now. In addition, Dina works as Lecturer at the Computers and Control Engineering Department, Faculty of Engineering, Tanta University-Egypt. She was born in the United Arab of Emirates, her B.Sc., M.Sc., and Ph.D. degrees taken from the Computers and Control Engineering Department-Faculty of Engineering, Tanta University in 2002, 2008, and 2014, respectively. Dina works as a Consultant Engineer, then a Database administrator, and finally acts as a Vice Manager on Management Information Systems (MIS) Project, Tanta University, Egypt, from 2008 until 2014. Her research interests include networking, wireless communications, machine learning, security, and the Internet of Things. Dina has published more than 42 articles in various refereed international journals and conferences. She is serving as a reviewer in Wireless Network (WINE) the Journal of Mobile Communication, Computation, and Information since 2015 Dina also acts as a Co-Chair of the International Technical Committee for the Middle East Region of the ICCMIT conference since 2020. (E-mail: d.hussein@qu.edu.sa, dina.mahmoud@f-eng.tanta.edu.eg).

Article submitted 2021-09-06. Resubmitted 2021-10-13. Final acceptance 2021-10-13. Final version published as submitted by the authors.