Data Encryption

Name

Institutional Affiliation

Data Encryption

**Introduction**

Encryption is a technique that is used to secure crucial data in the organization so that it does not become vulnerable to such things as hacking and malware attacks (Denis et al., 2021). The technique relies on transforming data into a unique code that can only be accessed by the use of a special key for encrypting and decrypting the data and thus this means that unauthorized individuals would have been prevented from having access to the data. “Data encryption can always prevent data loss especially when the data is at motion mainly because when data is at motion is when it is highly vulnerable to hacking attack” (Denis et al., 2021).

**Summary**

Data at rest means that the data is not being transmitted from one device to another. This means that the data is just stored within the computer or in a secondary device like an external hard drive (Denis et al., 2021). But still, there are high chances that someone can illegally gain access to data that is at rest, and a malicious individual can end up stealing the data or even manipulating or damaging it and at the end of the day, it is the organization that owns the data that will end up suffering data loss which might become very difficult to reverse the situation. “Data at rest does not mean that the data is secured as most people think (Denis et al., 2021).” We should always find a way of ensuring that the data at rest is secured from unauthorized access and the most significant way to achieve this is through the use of data encryption (Denis et al., 2021).

The basic is that the data at rest will be transformed into a unique code and stored in a computer or a hard drive and thus this means that even if an unauthorized individual happens to illegally gain access to the computer or the external hard drive he will not be able to read or manipulate the data that is at rest because it is unreadable when it is encrypted and anyone will need to have a key for decrypting it. “Hacking attack has become a big problem in this day and age, and thus organizations should begin accepting and integrating data encryption as the main way of securing their crucial information (Denis et al., 2021).”

Data in motion means that the data is being transmitted from one device to another and this is the moment when data is normally at a high chance of becoming vulnerable to hacking attacks. “When data is in motion is when it is highly vulnerable to attacks, so organizations should always take care (Dennunzio et al., 2021).” But on the other hand, data encryption can help solve this particular issue mainly because the data in motion will be transformed into a unique code that can only be decrypted by either the sender or the receiving using the key for decrypting the information. This key should never be given to anyone else except the sender or the receiver of the information.

Data in use can also be very much vulnerable to attacks especially malware and virus attacks because these are malicious programs that can get hidden in a computer system without the knowledge of the user and if the user happens to open a document a malware can easily delete, manipulate or damage the open document because the malware is programmed to harm documents and other crucial information in a computer system (Wen et al., 2021). First and foremost a user must always have antivirus and a firewall to secure his computer from virus and malware attacks and in addition to this, he should also encrypt all his documents so that they cannot be vulnerable to attacks. “It is better to stay safe always than to wait for attacks to take action (Wen et al., 2021).”

**Conclusion**

At this point in our lives, the internet and the advancement in technology has become a common thing in our lives and the main reason for this is because they have both played a crucial role in making our lives easier but on the other hand we should also acknowledge the fact that the internet has brought about a lot of threats in the society and this is the main reason why we should use data encryption to prevent data loss from unauthorized access. “Even though the internet has brought about a lot of opportunities into our lives, we should always consider securing our crucial information online (Wen et al., 2021).”

References

Denis, R., & Madhubala, P. (2021). Hybrid data encryption model integrating multi-objective adaptive genetic algorithm for secure medical data communication over cloud-based healthcare systems. Multimedia Tools and Applications, 80(14), 21165-21202.

Dennunzio, A., Formenti, E., Grinberg, D., & Margara, L. (2021). Decidable characterizations of dynamical properties for additive cellular automata over a finite abelian group with applications to data encryption. Information Sciences, 563, 183-195.

Wen, C., Li, X., Zanotti, T., Puglisi, F. M., Shi, Y., Saiz, F., ... & Lanza, M. (2021). Advanced Data Encryption​ using 2D Materials. Advanced Materials, 2100185.