**Summary of the Units**

This section will contain a form that will help represent the summary of information acquired from the previous three units. That is mostly based on system architecture, encryption, and a combination of security threats and other issues.

***Unit8***

The issues being encountered when looking at libraries involved in cryptography include the following based on the legal side of matters:

Export control – according to the US government, the application of cryptographic libraries and software requires that the involved party acquire the needed license for using the intended package and libraries.

Import control – this is where different states use different rules when it comes to how the libraries are being applied. This ensures that most of the security issues are meant for users to search for the appropriate method of abiding by the required law.

Patent related – this means that the libraries being used should at least be obtained through the required procedure. Or apply algorithms that are free from royalties to avoid infringement of a patent.

The application of cryptographic libraries in a system has both its benefits and drawbacks that are as follows:

**Pros**

Confidentiality – makes it easy for information to be protected from unauthorized access.

Authentication – the libraries make the information protected from issues like forgeries.

**Cons**

Most of the information that has applied strong encryption techniques is difficult to gain access to even with the legit user.

The application of these libraries can be found in the following areas:

* Secure communication occurs mostly between client and server programs in question.
* When storing data and also passwords.

***Unit9***

The ontology of distributed architecture in organizations and systems has made it possible for the information to be restructured in a way that makes it easy for it to be shared from one device to another with much ease.

***Unit 10***

Distributed architecture resulted from the need of clients to process more information due to the demand increase in technology. Through this many mobile operations from the client could be handle easily without putting much effort into the process of error handling that can be checked at the same time within the system that is distributed. The pros considered in this section looks at the following:

* Cost-effectiveness
* Efficiency
* Scalability

The cons on the other side involve the following :

* Startup cost
* Complexity
* Security issues

Security issues to be considered in this case when looking at virtualization include the following:

* Introspection exploitation – makes it easy for external observers to look at some of the stored data.
* Identity fraud – makes it easy for unauthorized disclosure to occur when not secured properly.

**Reference**

Haney, J.M., Theofanos, M., Acar, Y. and Prettyman, S.S., 2018. " We make it a big deal in the company": Security Mindsets in Organizations that Develop Cryptographic Products. In *Fourteenth Symposium on Usable Privacy and Security ({SOUPS} 2018)* (pp. 357-373).

Plejić, B., Šilić, M. and Golub, M., 2018, May. Stabile usage of export regulatory standards in data security process. In *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)* (pp. 1149-1154). IEEE.

Seth, B., Dalal, S., Jaglan, V., Le, D.N., Mohan, S. and Srivastava, G., 2020. Integrating encryption techniques for secure data storage in the cloud. *Transactions on Emerging Telecommunications Technologies*, p.e4108.

Sharma, P.K., Chen, M.Y. and Park, J.H., 2017. A software defined fog node based distributed blockchain cloud architecture for IoT. *Ieee Access*, *6*, pp.115-124.