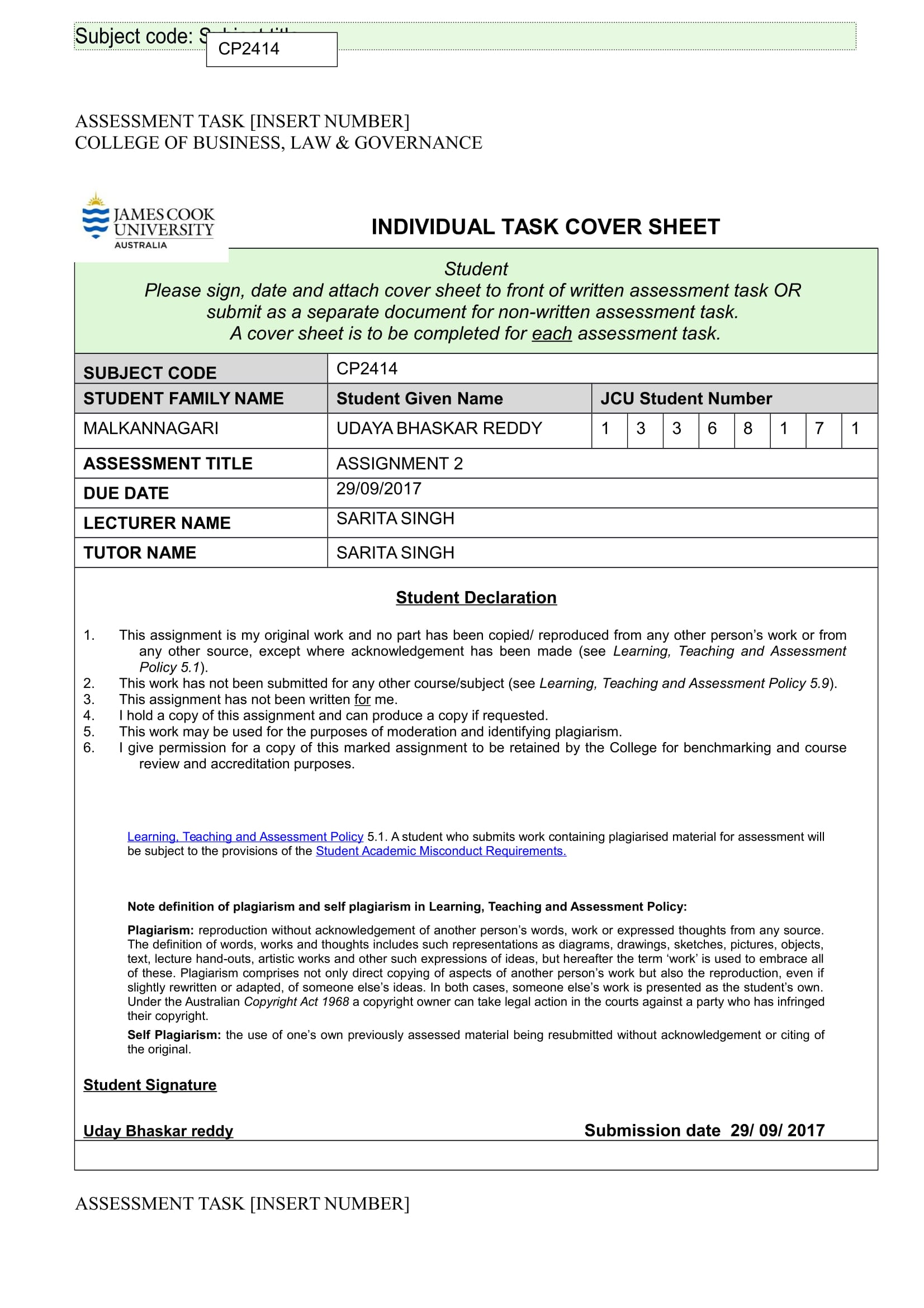
** Assignment 2**

**Cryptography and Network Security Applications – A case study**

**PART I: CRYPTOGRAPHY AND DATA SECURITY**

**Data Security:**

The company intends to license its logistics data to other companies and requires a secure way of sharing the information with its authorized partners. The company has never used any kind of data encryption methods before and looks at a comprehensive way of making its data secure. For this purpose, we can use various cryptographic techniques to protect the data from unauthorized disclosure and modification.

***What is Cryptography:***

Cryptography is a science of transforming information into a secure form so that no unauthorized users can access it. The data, as mentioned, is in its plaintext form. We can encrypt this data by changing the original text into secret message using Cryptography. Later on, we can decrypt the message back to its original form. The data that has been encrypted is called a Cipher text. Cryptography is more like a method of secret communication (the word *Cryptography* comes from the Greek word *kryptos*, which means hidden). Its main objective is to allow communication over an insecure channel so that a potential attacker may not be able to interpret what is being conveyed. For this purpose, different cryptographic algorithms are used to secure the information.

***Symmetric and Asymmetric Cryptography:***

Generally, Cryptographic algorithms can be categorized into three groups – Hash, Symmetric and Asymmetric. However, modern cryptosystems use a hybrid combination of these algorithms. These algorithms are also differentiated by the types of keys that are used for encryption and decryption methods.

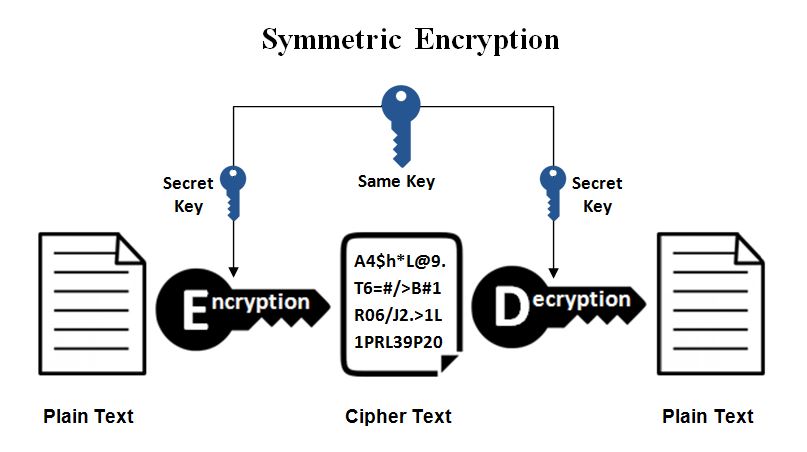
*Hash Algorithms:*

Hash algorithms create a unique digital fingerprint of data by a process called hashing. The fingerprint is called a message digest. Hashing is used primarily for comparison purposes. It is used to determine the integrity of the message. For example, digests are usually posted on the download sites so that a user can verify file integrity after the download.

*Symmetric Cryptography (private key cryptography):*

Symmetric Cryptographic algorithms use a same single key to encipher and decipher the message. A key here can be inferred as a mathematical value that is entered into the cryptographic algorithm to produce encrypted data. Unlike hashing, symmetric algorithms are designed to encrypt and decrypt the cipher text. Data encrypted by using this methodology will be decrypted when the receiver has the key. The primary challenge in this type of encryption is to get the key to the receiver. It is a process that needs to be conducted out of band, which implies that the whole process must be carried out on a channel other than the one carrying the cipher text. This will avoid any sort of interception that might happen otherwise. We can understand that it is necessary the key is kept private and confidential. For this reason, Symmetric Encryption is also called as Private Key Cryptography (book 1 reference).

The figure below illustrates the single key mechanism used in symmetric cryptography.



Symmetric Cryptography can provide strong protection against any sort of attacks as long as the key is kept secure. There are a number of symmetric cryptographic algorithms available which will be discussed in the later sections. Some of these popular encryption cryptosystems include,

* Data Encryption Standard (DES)
* Triple Data Encryption Standard (3DES)
* Advanced Encryption Standard (AES)

Symmetric Cryptography ensures protection on multiple layers. Its characteristics include protection of the confidentiality, integrity and availability of the information. However, it does not provide another key characteristic that will assure the authentication of a communication, which is non-repudiation. To ensure such a protective mechanism, we can use another form of encryption known as Asymmetric Cryptography or public key encryption.

*How Symmetric Cryptography can keep the company’s data secure?*

The implementation of symmetric encryption can provide a secure channel of communication between the company and its partners. We now look at a scenario wherein the company’s employees can interact and provide information to their authorized partners. For example, if a company’s employee, Eliza, wants to make a secure data transfer to their authorized partner, Bob. Eliza generates a secret key and shares it with Bob on a channel that is out of band to avoid any sort of interception (a channel other than the one carrying the cipher text). Once Bob has the key, Eliza can use it to encrypt the data, and bob can use it to decrypt it and read them. This will create a secure line of communication between the company and its authorized clients and partners.

Having such a mechanism in place will greatly increase the chances of protecting the confidentiality and integrity of the data in transit. Even though key distribution is a challenge, symmetric encryption is faster and its current standard algorithm, AES is extremely resistant against any form of brute force attacks. This algorithm has never been cracked yet and can be used as a protective mechanism to safeguard the company data.

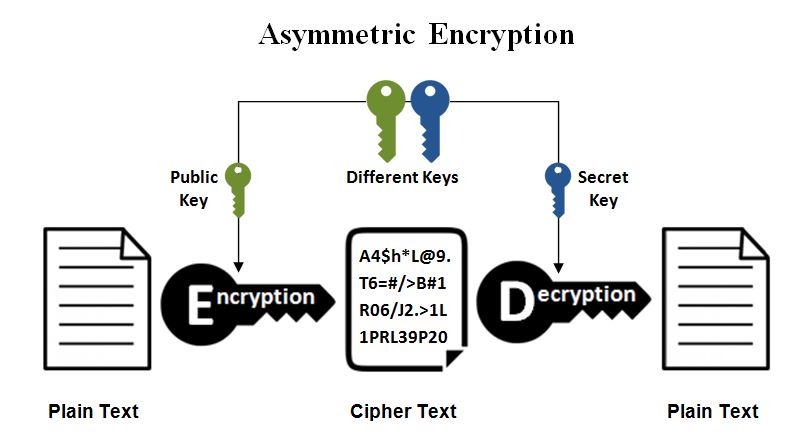
The company can also use symmetric cryptography to encrypt the emails within the organization. If there are emails that need to be sent securely, we can encrypt them using a symmetric cipher. We can also use this method to encrypt documents and files. The key that is used to drive the cipher can be extracted from a passphrase that is supplied when the file is encrypted. To add more security, this pass phrase should not be the same pass phrase that we use to protect the private key. Symmetric encryption is extremely useful in cases where the passphrase is not required to be communicated with others.

*Asymmetric Cryptography (public key encryption):*

The primary disadvantage of symmetric cryptography is the distribution and maintenance of a single secure key among many users. The problem is further escalated if the users are spread across various parts of the world, as is the case with the current company we are dealing with. To address this issue, we use another form of protective mechanism which is the asymmetrical encryption.

This is a relatively new method as compared to the symmetric encryption. In this type of encryption, we use two keys to encrypt the plaintext – a public key and a private key. The public key is freely distributed and made available to everyone who wants to send a message. The private key is known only to the person to whom it belongs. The data encrypted using a public key needs a private key to be decrypted. In the same way, the data encrypted using a private key can only be decrypted using the same public key. This mechanism will greatly enhance the security of the information that is being transmitted.

The figure below illustrates the different key mechanism used in asymmetric encryption.



Some of the protocols that use asymmetric cryptography for encryption include Secure Shell (SSH), open PGP and SSL/TLS. Many browsers use this mechanism to establish a secure connection over the internet or to validate a digital signature. The strength of the encryption directly depends on the key size. Increasing the key length will see an exponential increase in the strength of the encryption, however this might affect the performance. With the increase in computational power, more efficient algorithms will be used to create a more secure channel for data transfer.

*How Asymmetric Cryptography can keep the company’s data secure?*

The company’s CEO wants to share the data with their authorized partners. We now look at a scenario of how asymmetric cryptographic methods can help in securing the data. For example, if an employee at the company, Eliza, wants to send an encrypted piece of information to their authorized partner, Bob. Eliza will go to the public key registry and obtains Bob’s public key. As for asymmetric encryption, we know that the same key is not used to enciphering and deciphering the message. So, when we use Bob’s public key to encrypt the data, only Bob’s private key can be used to decrypt it. And that private key is only owned by Bob. In the same way, if Bob wants to respond to Eliza’s message, he can go to the public key registry to get Eliza’s public key and encrypt the data which can now be only be deciphered using Eliza’s private key. This is one of the most effective solutions to the key management issues that we face while using symmetric encryptions. It allows us to keep the private keys secret and share our public keys in reliable directories.

With such a mechanism, the company’s data can be securely shared with its authorized partners by using their public and private keys to encrypt and decrypt the relevant data.

Asymmetric encryption can also be used to encrypt the files in the company. As mentioned above, some of the protocols like SSL use asymmetric cryptography for encryption. There are also many desktop applications that are available which allow us to encrypt important documents or the emails that are being sent over the company’s intranet. It’s a simple mechanism that can be implemented by encrypting the email using the receiver’s public key the public key available under that application, and the receiving person can decrypt the email using their private key. This ensures a more secure channel of mail transfer.

**Message Authentication:**

Encryption is used as a means of protection against passive attacks like eavesdropping. Another requirement we look at is to have a protective mechanism against active attacks like falsification of the company’s data and their transactions with the clients. Protection against these kinds of attacks is known as Message Authentication. In addition to maintaining the confidentiality of the message, authenticating its contents comprises one of the most important security functions of the company’s network. It is a procedure that enables communicating parties to check and verify if the received messages are from an authentic sender and its contents were not altered. This is critical from the company’s perspective as confidential information needs to protected and transferred in an unaltered state to its clients.

It might seem plausible that authentication can be done by the simple use of shared key methodology in symmetric encryption. The sender and the receiver will have the same key, and we might assume that only the genuine sender has encrypted the message so that the recipient will recognize it as a valid message. In addition to that, a message included with an error-detection code, a sequence number or a time stamp will make it more authentic and genuine. However, this kind of encryption is not a suitable mechanism for data authentication. For example, when we analyze the ECB mode of encryption, an attacker can decrypt the message successfully by reordering the blocks of cipher text. It needs to be noted that such reordering may also alter the meaning of the overall message sequence.

Message authentication can be achieved with the use of authentication tags that are generated and appended to each message for transmission. This does not require encrypting of the message. However, it is possible to have a single algorithm that combines both authentication and confidentiality by encrypting the message along with its authentication tag. This technique involves the usage of a secret key mechanism to generate a small block of code, which is known as the message authentication code (MAC).

*What is MAC?*

MAC is short for Message Authentication Code. MAC provides both integrity and authentication of the data, and they achieve this based on a shared key mechanism as explained above. For example, if the company wants to send some data to its clients, the sender and the receiver will have a common key and in this way, when the receiver gets the message, he knows that this message has not been tampered with and it came from the sender with whom he shares a common key.

The technique is based on the assumption that the two communicating parties, A and B, share a common secret key, KAB. When a message is sent from A to B, the MAC is calculated as function of the message and the key.

MACM = F(KAB , M )

MACs are also referred to as keyed hash functions for which a secret key is needed for evaluation. One another important thing that needs to be noted is when a company’s employee A is communicating with a client B, and he is sending the message and the MAC, an eavesdropper can listen to this message as well as the MAC, but the eavesdropper cannot check the integrity of the message because the eavesdropper does not have the key. Only someone with the key can verify the integrity of this message.

MACs do not provide confidentiality and they require similar properties as hash functions like pre-image resistance, weak/strong collision resistance. In other words, if there is a message M which has a MAC, we should not be able to find another message which has the same MAC.

*Difference between MAC and Hash:*

We try to analyze the basic difference between a MAC and hash in providing security to the files. Suppose, if the company has an important file that is stored on its data disk drive, and they want to ensure that this file has not been tampered with, thereby we are also storing a hash of the file in the same directory. The procedure we follow to check the file was unaltered is that each time we want to use the file, we do the hash of the file and compare it with the stored value (let’s says, h). If the h value is the same, we assume that the file is not modified and if it differs, we will stop using that file. But there is a basic underlying problem of achieving security through this means. Because any attacker altering the file can potentially change the h value because hash is a public algorithm. They can modify the file and calculate a hash over it and change the h value. This implies when we are using the file, we are comparing the hash of the modified file with the changed h value and they will be the same.

As explained above, hashes have a limited functionality. But when we use MAC where a secret key is involved, it adds to provide a more secure means of protecting the data. We look at the same setup, where the company has an important file which is authenticated with a MAC. If an attacker were to alter the file, the attacker needs to have the key which they do not have. In other words, an attacker can never create a new MAC for a modified file without the key. This makes it better at ensuring the security of the file contents.

To summarize it all,

* A virus can modify a file and its hash also (recalculate). We cannot detect tampering
* A virus can modify a file but cannot calculate new MAC since it does not know the secret key

*How Cryptography can provide message authentication?*

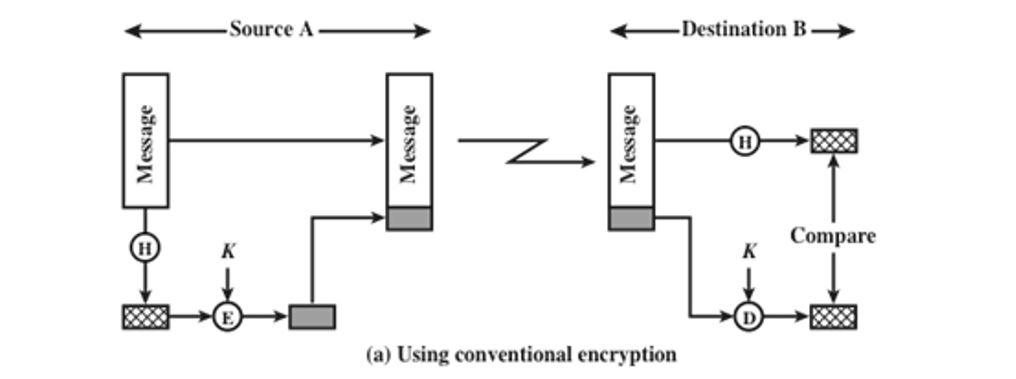
Message authentication can be provided by using the cryptographic techniques to encrypt data. A one-way hash function can be used as an alternative to the MAC. Just as is the case with the MAC, a hash function also accepts a variable size message (M) as an input which it uses to produce a fixed message digest H(M) as output. As explained earlier, the hash function does not use a secret key. In this case, the message digest is sent along with the message to verify its authenticity.

We now look at two ways the company can use to authenticate the message.

1. Using Conventional Encryption

This approach assumes that the sender and the receiver share the same encryption key. With such a mechanism in place, the authenticity of the message is assured as the client can use the key to decrypt the message and verify its authenticity. This is the most conventional approach to ensuring message security.

The figure below illustrates the way message is encrypted using the conventional means.



As we can see, the message is encrypted (E) at the source using the key (K) and later decrypted (D) at the destination using the same key (K) and then later compared for the hash value.

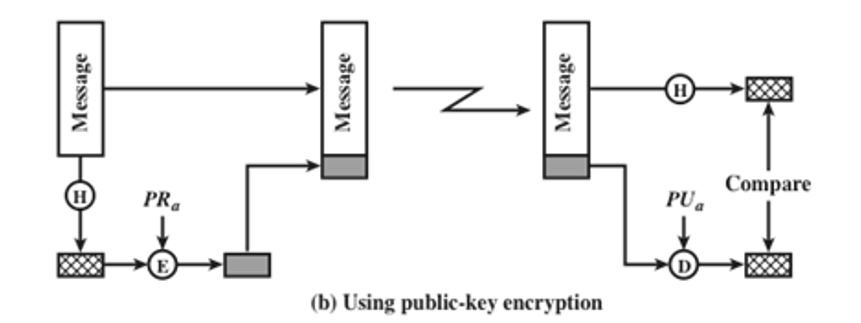
1. Using Public Key Encryption

This approach is based on the public key mechanism used in asymmetric cryptographic techniques. Here, the sender and the receiver use different public and private keys to encrypt and decrypt data as is the case with the public key cryptography. This approach has two primary advantages,

* + It provides us with a digital signature along with message authentication which greatly enhances security
  + Key distribution to communicating parties is not required.

As the public keys are already available in the public domains, it makes it easier to use them to encrypt the required data.

The figure below illustrates the public key encryption for message authentication.



One of the main advantages of using these approaches is that they require less computational power as against encrypting the entire message. There is a general opinion to avoid encryption altogether for specific reasons. Some of the reasons include,

* Encryption software being slower, despite the size of data being considerably small.
* Nonnegligible costs of Encryption hardware. Low cost chip implementation of DES is available. However, the costs will add up if all the nodes in the company’s network will require these capabilities.
* Normally encryption hardware is optimized for larger data sizes
* A patent can be used to protect the encryption algorithm

Depending on the company’s requirement, either of these methods can be used to ensure message authenticity.

**Cryptography Algorithm recommendation for Data Security:**

We now look at the cryptographic algorithm that is best suited to provide enhanced security to the company’s network. The main requirement is to have a secure channel of communication between the company and its authorized partners. We have analyzed the two different kinds of encryption techniques that are available for data protection – symmetric and asymmetric. We look at the current standards in these two techniques and try to judge the better of the available cryptographic algorithms that serve the company’s purpose.

*Symmetric Encryption faster than Asymmetric:*

Herein, we look at a model where the company’s employees share information with their clients on a secure channel. All these messages will be sent through the server. The communication between the two parties may happen several times a day. Messages will be of no fixed length and will be in plain text. The Sydney and Brisbane branches are provided with high speed internet and the traffic is also heavy throughout the week. So, we need encryption methods that require less computational power to provide a faster way of communication while encrypting and decrypting the data. The symmetric encryption can be considered relatively faster and less power hungry than an asymmetric mechanism especially when it comes to using large amounts of data. There are some asymmetric schemes like RSA with low public exponent that could approach the throughput of symmetric encryption, but we can say that atleast for decryption the symmetric schemes require less computational power.

*Size of the cryptogram:*

With symmetric encryption, we are not required to increase the size of the cryptogram asymptotically, which is not the case with asymmetric cryptography. We can take the example of RSAES-OAEP in PKCS#1v2. It has a 1024-bit key and a 160-bit SHA1 hash. A 1024-bit cryptogram can convey up to 688 bit of useful information. So, data enciphered this way can decrease the storage space by almost 49% and gain more time to move over a given link.

*Computational cost:*

The asymmetric algorithms are relatively computationally costly as compared to symmetric encryptions that provide equivalent security. The difference factor is the use of typically quite large keys. The public key methodology must be able to publish the encryption key without revealing the decryption key. This will require heavier mathematical calculations than the symmetric schemes.

We now look at the different algorithms that are provide the current standard in security and choose the best possible solution.

***Advanced Encryption Standard (AES):***

Symmetric cryptography provides strong protection against attacks as long as the key is kept secure. One of the first widely popular symmetric cryptosystems was the DES (Data Encryption Standard). It is a block cipher that divides the plaintext into 64-bit block sand and then executes the algorithm 16 times. The key had a length of 56 bits. DES was officially adopted as a standard for non-classified information by the US Government. But because of the short key size, it is no longer considered secure. It was later replaced 3 DES which is more advanced application of the DES. However, it was considered too weak to survive independently as the computing power continued to double every eighteen months.

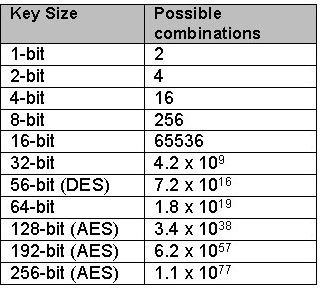
Advanced Encryption Standard (AES) is considered as a successor to 3 DES. It is a federal information processing standard (FIPS) that is used the US Government to protect data and information in federal agencies not part of the national defense infrastructure. It is approximately six times faster than 3DES.

Some of the features of AES include,

* It’s a symmetric key block cipher
* It has 128-bit data and 128/192/256-bit key sizes
* Faster than 3 DES
* It is software implementable in C and Java

As mentioned above, AES implements a block cipher called the Rijndael block cipher. This algorithm is based on several substitutions and linear transformations. This has a variable block length with 128, 192 or 256-bits key length. Technically, if we want to crack a 128-bit AES key with a state of -the-art supercomputer, it will take longer than presumed age of the universe. To date, no attacks have been successful against AES.

The following table illustrates the number of possible key combinations with respect to key size and how hard it is for a brute force attack to break the AES.



We now look at one of the current standard algorithms in asymmetric cryptography, RSA. It basically uses the two-key structure as discussed before where in the messages are encrypted and decrypted with different keys. This enables us to use another set of functions like the digital signatures which can verify the sender and also the integrity of the message. The security of this algorithm is based on integer factorization.

Although, we cannot directly compare the bit architecture of RSA and AES, a 2048-bit RSA is generally considered an equivalent to a 128-bit AES. The only way to crack the AES cipher is to try each and every possibility of the key until we reach the correct result. This can be termed as a Brute force attack. This implies that we can use enough bits in the key such that it can never be broken. However, RSA can be broken by factoring the modulus into primes and deriving the keys ourselves. It is a mathematical problem that can be solved to yield the right results. However, RSA is more advantageous in terms of key exchange but it is slow to use as compared to AES. But this makes AES more vulnerable to security risks of key exchange and distribution.

***Suggested Algorithm:***

Considering the abovementioned arguments and the company’s model suggested, we can conclude that a symmetric encryption mechanism like AES would serve well in providing a secure communication channel with the company’s clients. AES is faster, demands less computational power and is highly resistant against any form of brute force attacks. These requirements must be met as the company’s branches are already under heavy load of heightened network traffic. The company can share the secret key with its authorized partners and use it to encrypt and decrypt the required information. Such a simple mechanism will be beneficial even while protecting the files within the organization. Emails and data files can be encrypted using the AES ciphers to make them more secure and confidential.

**Cryptography Algorithm recommendation for Message Authentication:**

Message authentication in programs and applications can be achieved with the help of one-way cryptographic hash algorithms. The one-way hash function also known as the secure hash function provides message authentication along with message integrity with the aid of digital signatures. To understand the mechanism of implementation of hash algorithm, we need to understand what a hash is.

*What is a hash?*

A hash function is a mathematical algorithm, which will return a unique output (hash) for any unique input content. The content can be a document, file, sound, video or a picture. The primary purpose of this function is to produce a “fingerprint” of a file or any block of data. To serve its purpose for message authentication, a hash function must exhibit several characteristics. Some of these include,

* We can apply hash to a block of data of any size.
* A fixed-length output is produced by the hash.
* It is easy to compute H(x) for any given x, which makes it practical to implement it in both hardware and software.

Some of the other properties include the hash function being pre-image resistant, weak collision resistant and strong collision resistant.

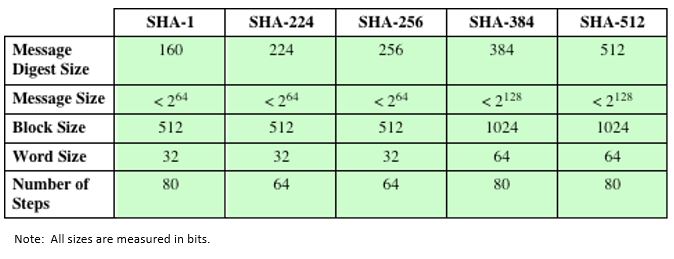
*Hash attacks*

The strength of a hash lies within its ability to deliver the same unique output to all the submitted unique content. Along with that, anyone getting the unique output should not be able to create the original content submitted to create the has result simply from the hash result only. This is called a preimage attack and as mentioned above, a hash function should be preimage resistant. Hashes are generally considered secure at their inception but overtime, the attackers devise several ways of using math to exploit and weaken its protective strength. Attackers used cracked hashes as malware to fake legitimate digitally-signed software.

*Hashing Algorithm (SHA):*

SHA or Secure Hash Algorithm is a family of hashes. The first version, SHA-0, was withdrawn due to a flaw after release. Later SHA-1 which was developed in the year 1993 by US National security agency and NIST (National Institute of Standards and Technology) became a standard for hashing algorithms. SHA-1 creates a digest of 1160 bits. The current standard used SHA-2 is considered more secure and it comprises a total of six variations – SHA-224, SHA-256, SHA-384, SHA-512, SHA/512/224 and SHA-512/256. The last number in these algorithms indicate the length of the digest in bits.

The following table gives us a better understanding of the parameters involved.



*Reasons for recommending SHA-2 as the selected algorithm for message authentication:*

We now look at the company’s perspective and how secure a hash algorithm can be in providing message authentication. As is the case with symmetric encryption, we have two ways of attacking a secure hash function – cryptanalysis and brute-force attack. These attacks try to exploit the logical weaknesses in the algorithm. Furthermore, the strength of the hash function against these attacks is dependent on the length of the hash code which the algorithm produces. For example, another hash function MD5 with a 128-bit hash length is considered inadequate as compared to a hash functions with a longer hash code. We can now clearly see the implementation of a greater secure mechanism provided by SHA-2 with variable hash code lengths as displayed in the table above.

We now look at the case of password storage and how the hashing algorithms respond to it. If the company wants to authenticate some confidential data with strong password protection, they have to implement the best scheme that can resist any attacks. SHA-1 provides a collision-resistant hash of given input as fixed-length output. SHA-2 was specifically designed in such a way that it can overcome the theoretical breaks of SHA-1. This new design increases collision resistance thereby improving security. An attacker will require more time to hack a SHA-2 algorithm. We can safely say that, when it comes to collision resistance, SHA-2 is more secure than SHA-1. Even in the case of brute force attacks and dictionary-based attacks, the attacker will take more time to find the unique passwords the authentication routine will verify. However, it must be noted that these attacks do not seek collisions to authenticate attackers. The attacker will try various combination of passwords and hash them with the chosen algorithm until the password corresponding to the stolen hash is found. All in all, it needs to be understood that increased collision resistance of SHA-256 and SHA-512 will produce longer outputs (256b and 512b) than the SHA-1(160b) making them more attack resistant. This will make SHA-2 a better option to provide password security to the company through message authentication.

We also look at the case of how hashes are used in SSL certificates. The company can use the SSL/TLS protocol to enable a secure transmission of information across the internet. As mentioned in the earlier sections, SSL provides encryption. Along with that, it also provides authentication which tie to the SSL certificates that connect a public key to an identity. Digital signatures form an important part of providing authentication through SSL certificates. They provide us with a cryptographic proof that the SSL certificate has been signed by a certifying authority (CA) and it has not been modified or altered. To check these signatures quickly, the CA hashes the certificate and later signs the resulting hash. The security of these digital signatures depends on how collision resistant the hashing function. This makes SHA-2 an obvious choice.

The encryption hash that is used in SHA-2 is significantly stronger and is made secure from all the vulnerabilities that were found in SHA-1. However, there are some drawbacks that need to be considered when choosing this algorithm. As compared to MD5 and SHA-1, the computational speed and performance of SHA-2 is relatively slower. But it needs to be noted that MD5 and SHA-1 are already compromised and are not considered secure anymore. And the company is looking at a more secure mechanism rather than a faster solution, and based on the context, it has a highspeed network that will enable for a faster transmission of data making SHA-2 as the best choice for message authentication.

**Digital Signature:**

A digital signature is a cryptographic transformation of data which provides a methodology for the verification of source authentication, message integrity, and signatory non-repudiation. It is a bit pattern that is dependent on the data. It is generated by an agent as a function of a file, message or any other form of data block. This mechanism can be used by verification by another agent. They can verify the data block for its associated signature to check,

* If the alleged signatory has signed the data block.
* If the block of data has not been modified since it is signed.

In this way, the signer will not be able to repudiate the message.

There are three digital signature algorithms which the FIPS 186-4 specifies to use,

* Digital Signature Algorithm (DSA), based on computing discrete logarithms
* RSA Digital Signature Algorithm, which relies on the RSA asymmetric algorithm
* Elliptic Curve Digital Signature Algorithm (ECDSA)

*Implementation of the digital signature model for the company:*

We now look at a model that the company can make use of using digital signatures. Suppose, if the company’s employee, Eliza, wants to send a message to a client, Bob. And she wants Bob to be certain that the message came from her. She uses a secure hash function, SHA-512 as mentioned in the previous section, and generates a hash value for the data. This hash value along with Eliza’s private key will serve as an input to the digital signature generation algorithm. A short block is produced which serves as a digital signature. As the client, Bob, receives the message, he calculates the hash value for this data and provides the hash value along with Eliza’s public key as inputs to the digital signature algorithm. If the algorithm returns a positive result that the signature is valid, Bob will be assured that the message has been signed by Eliza. As Eliza’s private key cannot be accessed by anyone else, Bob will be assured that the message has not been modified or tampered with during the transit.

However, it needs to be noted that the mechanism described above does not provide confidentiality of the message. The message will remain in an unaltered state, but not completely safe from eavesdropping. This problem can be addressed by use of cryptographic algorithms suggested in the previous sections. And the company can use this model to assure its clients and partners that the data sent is from the actual source and its contents have not been altered.

*RSA Digital Signature Algorithm:*

RSA Digital Signature Algorithm is one of the recommended solutions for digital signature methodology. It encrypts the hash of the message that is to be signed using RSA. Just as is the case with RSA encryption algorithm, the digital signature algorithm first modifies the hash value to improve security. This can be done in several ways, one being the RSA Probabilistic Signature Scheme (RSA-PSS). When an attacker tries to find another message or two messages which map to the same message digest as the given message, this algorithm will make the whole process more difficult. Because signing the message which uses the same private key more than once will yield different signatures as the salt changes with every use. This will work as an added measure of security.

**PART II: CRYPTOGRAPHIC KEY AND USER AUTHENTICATION**

**User Authentication:**

The company has grown multifold overtime and wants to avoid a scenario where fake users may access their network resources. The company wants a comprehensive user authentication mechanism that enables it to counter any such intrusions.

User authentication can be considered as a primary line of defense in providing computer security. It provides the basis for user accountability and access control. It is a basic step to verify the identity of the user or the system that is accessing the network. There are two steps that serve this purpose – Identification and Verification.

We can analyze these two steps in a closer detail and see how it can be implemented within the company’s network. Basically, identification involves presenting an identifier to a security system like passwords or the use of biometric scanner. Verification, on the other hand, enables us to present or generate authentication information that corroborates the binding between the entity and the identifier. In other words, it’s a confidence building technique that identifies the user’s credentials when they are presented electronically to a security system. This allows the system to determine if the authenticated user is allowed to perform certain tasks and functions on the network. This authentication and authorization mechanism can be implemented within the company’s local area network as well.

*Authenticating a user’s identity in the company’s network:*

We can employ several different means to authenticate a user’s identity in the company’s network. We look at four different ways this can be done. All the methods can be used as a standalone variant or in combination to each other.

*Something the individual knows*: This includes the passwords, personal identification number (PIN) of the employees, or the answers to a prearranged set of questions.

*Something the individual possesses*: This includes distribution of cryptographic keys, electronic keycards, smart cards and physical keys to the company’s employees so that they can have access to secured layers of data. This can be referred to as token authentication.

*Static Biometrics*: This method involves physical recognition techniques like fingerprint, retinal and face scans. This enables identifying the users quite easily.

*Dynamic Biometrics*: This involves recognition of voice patterns, handwriting characteristics and typing rhythm.

All these approaches can be implemented within the organization to allow for more secure mechanism in authenticating user credentials. However, it needs to be noted that each of these methods have their own flaws- passwords can be stolen or forgotten, tokens can be lost, biometrics can produce errors. And more of the company’s resources may be required to be spent on monitoring these systems. For a network-based user authentication, we can use the cryptographic key mechanism as a viable alternative.

***Recommendation for user authentication – Kerberos:***

*How keys are distributed?*

The strength of any cryptographic system rests on its key distribution technique. If the company uses symmetric encryption, the two parties must exchange the same key and protect it from outside access. There are multiple ways in which key distribution can be achieved.

* A key could be selected and physically delivered to the client
* A third-party service can be used to physically select the keys between the two entities communicating
* If both the parties have previously used a key, one entity can use the old key to provide encryption of the new key and transfer it safely
* If both the parties have an encrypted connection to a third party, the third party can deliver the key on its encrypted links to both the parties.

As mentioned above, it can be done manually by physically delivering the key to the company’s clients or other parties. However, for end-to-end encryption of data over a network, this kind of manual delivery is awkward and inefficient.

*Types of keys used:*

The company requires a model where two end systems are required to communicate on a logical connection. In this case, a session key is a viable option. The session keys will be destroyed after each session is completed. Along with this, a permanent key can be used between these two connecting entities for distributing session keys. This can be achieved with the help of key distribution center (KDC), a third-party authentication service. In this case, a master key is shared by both the end systems and a permanent key is used to encrypt the session key through the duration of the connection. This kind of automated key distribution provides a more flexible and dynamic functionality in allowing exchange of data between two channels. Kerberos is one of the most widely used applications that implements this functionality.

*Type of Encryption used in Kerberos:*

Kerberos is a network authentication protocol which uses symmetric encryption techniques to provide a secure authentication for client/server applications. It can be used to authenticate and authorize service requests between the company’s hosts and its trusted clients across the internet. IT is developed at the Massachusetts Institute of Technology (MIT). It relies completely on symmetric encryption making no use of public-key encryption.

*How the keys are employed in the process:*

The word Kerberos is derived from the Greek mythology, Cerberus, a three-headed dog that guarded the gates of Hades. It’s an analogy we can use to refer to the three head of Kerberos – client, server and the KDC. The Kerberos server database will have the user information of all the registered users in its database. Also, each server must share a secret key with the Kerberos server and all the servers are registered with the Kerberos server.

We now look at a model where an initiating client is trying to logon to the company’s network.

The client sends a request to the authentication server for accessing a service. The server retrieves the private key of the client and checks for the client’s username in the KDC database. The process stops here if no name is found. If the username is found in the KDC database, the server generates a session key along with a ticket granting token. This token will be timestamped and encrypted by the server with the client’s password. The client will now be required to enter a password which should match with the one in the KDC database. The token will now be decrypted and used to request a credential for the required service from the ticket granting server.

The ticket granting service undergoes the same process as the authentication server, and sends the credentials and a ticket to access the desired service. A session key will be used to encrypt this transmission between the user and the service being accessed. The timestamped ticket implies that the service can only be accessed for a specific period of time on a single time. This will reduce the risk of someone using the ticket later at another time. The maximum lifetime of the tickets can also be set to 0 which make the service tickets not expire. Microsoft suggests a lifetime of 600 minutes for these service tickets which is used as a default value for Kerberos.

*Advantages of Kerberos:*

An unauthorized user can perform several functions like eavesdrop on exchanges, and use a replay attack to gain access to the server or alter the network address of a host to send malicious requests from the impersonated host computer. Instead of building an elaborative mechanism to stop such intrusions at every server, Kerberos acts as a centralized authentication server whose primary function will be to authenticate clients to servers and servers to clients.

*Kerberos 4 and 5:*

Kerberos 4 makes use of DES to provide authentication. The version 4 has many limitations which made it unreliable due to the advancement of emerging technologies. This made the transformation to Kerberos version which addresses the said limitations in two areas – environmental shortcomings and technical deficiencies. These shortcomings include, ticket lifetime, message byte ordering, internet protocol dependence encryption system dependence to name a few. Along with these, technical deficiencies like session keys, password attacks were also addressed in version 5.

All in all, we can conclude that Kerberos can be used as a secure protocol to provide user authentication to the company’s services.

**User Authentication – Passing Employee Identities to the trusted parties**

The company CEO wants to extend the employees’ benefits by giving discounted prices on fruit juices and nut bars. The URLs of both these companies, [www.ijuice.com](http://www.ijuice.com) and [www.nutbar.com](http://www.nutbar.com) will be added on the employee benefit page. These links will be accessible only to the employees upon signing on to the company system. When the employees click on these links, the employees’ identifier will be passed on to the juice and nut bar websites. This must be done in a secure manner.

*Recommendation for user authentication process and passing employees’ identities to the trusted parties:*

We now look at a relatively new concept, Federated Identity Management, which can aid the company in having a common employee identity management scheme across multiple domains and numerous applications. It’s an arrangement that can be made among multiple enterprises, in this case the company and the different product websites, to let employees use the same identification data that allows access to these websites in the federated group. To understand this, we first need to get an overview of the concept of identity management in general.

Identity management is a centralized, automated approach to provide enterprise wide access to resources by employees and other authorized individuals. Herein, we define an identity for each employee in the company, we associate several attributes to them like their phone number, account number, billing info etc., and enforce a means by which their identity can be verified. The central idea for this kind of a verification methodology involves a single sign-on (SSO). SSO allows the employee to access all the network resources with a single authentication.

Some of the services that are provided by a federated identity management system are listed below. We look at them from the company perspective and try to interlink the services together to provide an authentic mechanism to validate the employees’ identities.

Point of contact: This includes the authentication mechanism that an employee corresponds to the user name provided and the further management of user/server sessions.

SSO protocol services: This is critical to a federated management system as it provides a vendor-neutral security token service for supporting a single sign on to the specific websites.

Identity services: These services are important as they provide an interface to the local data stores which include employee registries and databases. This can be used for identity related information management.

Trust Services: Trust is critical ingredient in building a stronger federation relationship. This can be a combination of security tokens used to exchange employee information along with the cryptographic information used to protect these security tokens.

*How does this solution work?*

To understand how this solution works, we need to get an overview of what an identity federation is. Identity federation is more like an extension of identity management to other security domains. The company along with its website partners will form a federation of trusted entities. The goal is to provide sharing of digital identities so that an employee can be authenticated a single time and then can have authorized access to the website for buying the discounted products. This cooperation is based on mutual trust between the organizations to securely share the digital identities of the users. As discussed in the previous sections, the trust services form a core part of these federated groups. The employee can log on to the company’s intranet and be authenticated to perform authorized functions and access authorized links to these websites. The employee can buy the discounted juices and nutbars without having to re-authenticate.

Federated Identity management also provides other capabilities. This relates to the way how attributes are represented. Different kinds of attributes can be added to the employees’ identities like passwords, biometric information, organizational roles, location, etc., to name a few. The employee can also have multiple identifiers. In such a case, each identifier will be associated with a unique role with its own access permissions. Another key advantage of federated identity management is to have identity mapping. This makes mapping of the employee identity across several domains much simpler irrespective of the domain architecture.

The whole scenario of how the employees use this service is explained briefly below.

The company contracts with juice.com and nutbar.com to provide discounts on products to the employees. The employee uses the web interface to sign on to the company’s network and goes through an authentication procedure there. This enables the employee to access authorized services in the company’s network. When the employee clicks on the links to either of these websites, their browser will be redirected to these websites. At the same time, the company’s software passes the user’s identifier to the website in a secure manner. The company and the websites are part of a federation that can exchange user identifiers securely. The website organizations maintain user identities for every employee working at the company and associates with each identity health-benefits information and access rights. This linkage between the two companies is based on account information and the employee participation is browser based.

**PART III: EXPLORE SECURE CLOUD COMPUTING FOR HANDLING THE COMPANY’S DATA**

*How to implement Cloud computing for the company’s valuable data?*

Cloud Computing is an on-going evolution of business connectivity and activity. In simpler terms, it’s an off-site storage of company data that is made accessible from any location across numerous platforms through internet access. Instead of storing the data on the company office hard drives, the information is made available by uploading it to a cloud. We now look at the scenario wherein the company can benefit from employing cloud computing for its valuable data.

In technical terms, the NIST defines cloud computing as a model which enables ubiquitous, convenient and on-demand network access to a shared pool of configurable computing resources. We can understand how these services could be implemented in a typical cloud service context. The company maintains a set of workstations within its local area network. These LANs will be connected to the network through a router to the cloud service provider. This cloud service provider will maintain a large collection of servers which are managed effectively and securely through a variety of management, redundancy and security tools. The Cloud Provider (CP) provides the storage and the processing facilities needed to support the company’s data. There are also value-added services like identity management performance reporting, optimizing performance and minimizing the costs which can be done with the aid of a cloud broker.

*What Cloud Computing services can be used for the data?*

There are three different models that provide a layered architecture in delivering cloud computing services. We can look at how the company can use these service models within their organizational framework.

*Software as a service (SaaS):* In this model, we are provided access to software applications. This can be referred to as “On-demand software”. The company is not required to worry about the installation, setting up or running of the application. The cloud service provider will do that job for it. The clients and users will be able to access all these services offered through the cloud provider. The applications will be available from various client devices through a thin client interface like a web browser. This service helps in saving from the complexity of software installation, upgrading and maintaining it regularly.

Some of the popular examples of such services include Google Apps, Gmail, Salesforce.com and Microsoft 365

*Platform as a service (PaaS):* This service as the name suggests provides all the computing platforms as services. This offers the clients more control than the basic services offered through SaaS. These platforms include operating system, programming language execution environment, database, web server etc., based on the company’s choices to share its valuable data. PaaS is basically an operating system on the cloud.

Some of the examples of this service include AWS Elastic Beanstalk, Google App Engine, Heroku to name a few.

*Infrastructure as a service (IaaS):* This service provides the computing infrastructure, physical as well as virtual machines like virtual disk image library, firewalls, IP addresses, load balancers, VLANs etc., as cloud services. This gives the user utmost control over the data available. The company can provide these services to the clients enabling them to deploy and run arbitrary software.

Some of the examples include Amazon EC2, Google Compute Engine.

The company can decide which of these services it can use to store their data using the cloud computing services.

*What are the Cloud security risks and countermeasures?*

The security controls employed in cloud computing are similar to any other security controls in any IT environment. However, because of the various technologies and models used to enable cloud service, there may be several risks that need to be looked at.

The cloud security alliance (CSA10) gives a list of several risks a cloud computing environment faces and their counter measures.

*Abuse and nefarious use of cloud computing:*

When we look at some of the cloud services where free limited trial periods are offered, the attackers can use this to their advantage to conduct various attacks which include spamming, DoS, malware injection to name a few.

Countermeasures for this include,

* a validated login mechanism
* a thorough introspection of customer network traffic
* a more secure credit card fraud monitoring and coordination
* having public blacklists and monitoring them regularly.

*Malicious insiders:*

By using the cloud computing services, the company will relinquish direct control over many aspects of securing the various applications and software’s and puts the entire trust of the service provider. This puts us at a grave risk of insider activity that might compromise the company’s network.

Countermeasures include,

* Enforcing a strict supply chain management and conducting a comprehensive supply chain assessment.
* Along with that, we can specify human resource requirements as part of a legal contract.
* Enable a transparent mechanism in the management practices, and also create a mechanism that determines security breach notification processes.

*Insecure interfaces and APIs:*

The basic user interfaces and APIs that the cloud providers expose must be secured against any malicious attempts to circumvent their security policies.

Countermeasures include,

* A basic analysis of the security model of these user interfaces
* Implementing strong authentication and access controls with encrypted transmission
* Gaining an understanding of the dependency chain associated with the API

*Data loss or leakage:*

Data loss because of security breach can deliver irreparable damage to the company

Countermeasures include,

* Implementation of a stronger API control
* Protecting the data in transit by encryption
* Implementing a strong key generation, storage and management practices

*Account or Service hijacking:*

Attackers can steal the credentials of the users and compromise the confidentiality and integrity of these services.

Countermeasures include,

* Prohibiting the sharing of these account credentials
* Use a more secure two factor authentication mechanism
* Monitor unauthorized activity by proactive means

**Cloud Computing Recommendation:**

We have looked at several risks and their countermeasures that can help in delivering a comprehensive understanding of how the cloud computing services work. Now, we look at the advantages the company can have by using these cloud services.

Firstly, we look at the security angle of protecting data. As the company is expanding it will have to take extensive measures to protect is data from hackers. Employing cloud computing services that provide good security measures can be looked at as an alternative to protecting the data. It’s a two-layered architecture where in data is secured by the company’s own security mechanism along with the cloud security. The high levels of encryption that modern day cloud services provide can greatly enhance the security of the organization.

Secondly, using a cloud service to store data will make collaboration easy and boost employ and client confidence. As the data is readily available on a secure site, working on multiple projects become much simpler. Collaboration among clients, employees, outsourcing professionals becomes much simpler as each individual entity will be having a different set of privileges to data access.

Thirdly, Information is readily available on the go. If the company has to deal with activities from different time zones over extended periods of time, the cloud services will really help in making the data readily available at all times.

Fourthly, if any natural disasters like earthquakes or flooding happen that disrupt the functioning of the company for a certain period of time, having cloud services allow to have a continuity to the organization’s functioning.

Lastly, Cloud computing is affordable and scalable. Instead of shelling out a lot of money on security services, cloud security can be used as a safer and reliable means of protecting data. It can also operate cross platform. We can use any digital service to access the data from the cloud provider.

*Cloud Security as a Service (SecaaS):*

By analyzing all the benefits and counter-benefits of using a cloud service, we can safely conclude that the company can employ a cloud computing service to share its data. To implement this mechanism, the company can incorporate cloud security as a service for enhanced security. SecaaS is a segment of SaaS provided by the cloud service. It is provided as a package to a service by the cloud provider to reduce the security burden on the company. Several services like authentication of user credentials, antivirus and antimalware software, IDPS, security event management are offered under this service.

The SecaaS categories of services offered include,

* Data loss prevention
* Email security
* Web security
* Security assessments
* Intrusion management
* Identity and access management
* Encryption
* Business Continuity and disaster recovery
* Network security

The company can employ any of the cloud services offered based on the organizational requirements and also take the SecaaS as a security mechanism to protect its valuable data. It’s a cost-effective mechanism that can provide multiple benefits to the organization’s functioning.

**PART IV: BUSINESS AND BLOCKCHAIN INTEGRATION**

*How Blockchain can be integrated into the business for transactions:*

The blockchain technology is a new ingenious invention that has the potential to revolutionize the digital world. It is a distributed database of records and acts like a public ledger of all transactions. Participating parties can share and execute digital events among themselves. Once the information is entered, it can never be deleted. This allows for a verifiable record of every transaction that was ever made.

The company can use the services of this new and innovative technology to store information. Information on the blockchain exists as a shared database. This database will be constantly updated across all the networks its being shared. There is no centralized mechanism that allows a hacker to corrupt a piece of data.

We can take the example of google docs and how sharing and editing of the document has revolutionized the idea of collaborative documentation. People can access these docs simultaneously and edit it at the same time.

We can list two important characteristics of block chain – distributed consensus and anonymity. Blockchain has been successfully applied to both financial and non-financial markets. A popular example of its usage in the financial applications is the peer to peer electronic cash system – bitcoin.

Blockchain technology is transparent and incorruptible. Altering a small piece of information on the blockchain will require a large amount of computing power to override the entire network. This will reduce the risk of data corruption. Also, blockchain technology is durable and robust. It cannot be controlled by a single entity and has no single point of failure.

*Advantages and disadvantages of employing blockchain with the company’s transactions:*

We now look at the benefits of using the blockchain technology for the company’s transactions.

***Advantages:***

*Disintermediation and Trustless exchange:*

The company will be able to make an exchange with its clients and other partners without the intermediation of a third party. This greatly reduces counter-party risk.

*Empowered users:*

Users are in control of all the information and transactions.

*High quality data:*

Blockchain provides a data that is complete, timely and widely available.

*Durability, reliability and longevity:*

As there is no centralized control, blockchains does not have a single point of failure.

*Process Integrity:*

Clients can trust that transactions will be executed as declared by the protocols without any third-party interference.

*Faster Transactions:*

Blockchain transactions can basically reduce the interbank transactions to minutes as compared to the normal transactions.

*Lower transaction costs:*

Costly will be greatly reduced as there will no third-party intermediaries involved.

***Disadvantages:***

*Nascent technology:*

As this is still a nascent technology, challenges like verification process and data limits have to addressed to make kit more efficient in the future.

*Large energy consumption:*

It requires substantial computational power

*Control, security and privacy:*

As the company must entrust its private data to a blockchain solution, the system has to be made more secure and protective against any form of cyber security attacks.

*Integration concerns:*

Company’s applications require significant changes to be made in order to be integrated with the Blockchain applications.

*Costs:*

Initial capital costs are considerably high.

All in all, by looking at the both the benefits and challenges of the blockchain technology, it can be safely said that the company can use this innovative technology as a means of sharing and securing its transactions. The current evolving trends in the digital world will further increase the functionality of this existing system making it more secure and user-friendly.

**References:**

1. Whitman, M. E., & Mattord, H. J. (2016). *Principles of information security* (Fifth ed.). Boston MA: Cengage Learning.
2. Dean, T. (2012). *Network+ guide to networks (with printed access card)* (6th ed.) Wadsworth.
3. Stallings, W. (2011). *Network security essentials: applications and standards.* Boston, MA: Pearson
4. Northcutt, S. (2005). *Inside network perimeter security.* Indianapolis, IN: Sams Pub.
5. S. W. (1969, May 01). What is Blockchain Technology? A Step-by-Step Guide For Beginners. Retrieved September 29, 2017, from <https://blockgeeks.com/guides/what-is-blockchain-technology/>
6. What is Blockchain Technology? A Step-by-Step Guide For Beginners. Retrieved September 29, 2017, from <https://blockgeeks.com/guides/what-is-blockchain-technology/>
7. What is federated identity management (FIM)? - Definition from WhatIs.com. (n.d.). Retrieved September 29, 2017, from <http://searchsecurity.techtarget.com/definition/federated-identity-management>
8. What is federated identity management (FIM)? - Definition from WhatIs.com. (n.d.). Retrieved September 29, 2017, from <http://searchsecurity.techtarget.com/definition/federated-identity-management>
9. What is the Difference Between SHA-1, SHA-2 and SHA-256? Retrieved September 29, 2017, from <https://www.thesslstore.com/blog/difference-sha-1-sha-2-sha-256-hash-algorithms/>