Multipurpose Internet Mail Extensions (MIME)

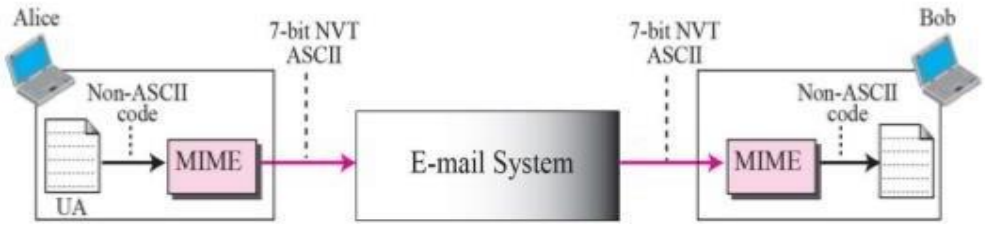
- **Multipurpose Internet Mail Extension (MIME)** is a standard which was proposed by BellCommunications in 1991 in order to expand limited capabilities of email.
- MIME is a kind of *add on or a supplementary protocol* which allows non-ASCII data to be sentthrough SMTP. It allows the users to exchange different kinds of data files on the Internet: audio, video, images, application programs as well.

- **Why do we need MIME?**

Limitations of Simple Mail Transfer Protocol (SMTP):

1. SMTP has a very simple structure
2. It's simplicity however comes with a price as it only send messages in NVT 7-bit ASCII format.
3. It cannot be used for languages that do not support 7-bit ASCII format such as-French, German, Russian, Chinese and Japanese, etc. so it cannot be transmitted using SMTP. So, inorder to make SMTP more broad we use MIME.
4. It cannot be used to send binary files or video or audio data.

•MIME was designed mainly for SMTP, but the content types defined by MIME standards are also of importance in communication protocols outside of email, such as Hyper Text Transfer Protocol (HTTP) for the World Wide Web.



MIME *transforms non-ASCII data* at sender side to NVT 7-bit data and delivers it to the client SMTP. The message at receiver side is transferred back to the original data. As well as we can send video and audio data using MIME as it transfers them also in 7-bit ASCII data.

S/MIME (Secure/Multipurpose Internet Mail Extensions)

- S/MIME is an extension of the widely implemented Multipurpose Internet Mail Extensions(MIME) encoding standard
- S/MIME uses the RSA public key cryptography algorithm along with the Data EncryptionStandard (DES) or Rivest-Shamir-Adleman (RSA) encryption algorithm.
- S/MIME provides the following functions:
- ● **Enveloped data:** This consists of encrypted content of any type and encrypted-contentencryption keys for one or more recipients.
- **Signed data:** A digital signature is formed by taking the message digest of the content to besigned and then encrypting that with the private key of the signer. The content plus signature are then encoded using base64 encoding. A signed data message can only be viewed by a recipient with S/MIME capability.
- **Clear-signed data:** As with signed data, a digital signature of the content is formed. However, in this case, only the digital signature is encoded using base64. As a result, recipients without S/MIME capability can view the message content, although they cannot verify the signature.
- **Signed and enveloped data:** Signed-only and encrypted-only entities may be nested, so that encrypted data may be signed and signed data or clear-signed data may be encrypted.

■ **Must:** The definition is an absolute requirement of the specification. An implementationmust include this feature or function to be in conformance with the specification.

■ ● **Should:** There may exist valid reasons in particular circumstances to ignore this feature or function, but it is recommended that an implementation include the feature or function.

➢ MOBILE DEVICE SECURITY

Mobile Device Security refers to the measures designed to protect sensitive information stored on and transmitted by laptops, smartphones, tablets, wearables, and other portable devices. At the root of mobile device security is the goal of keeping unauthorized users from accessing the enterprise network. It is one aspect of a complete enterprise security plan.

- Lackof Physical Security Controls

Mobile device is required to remain on premises, the user may move the device within the organization between secureand non secured locations. theft and tampering are realistic threats.

The threat is two fold:

1. A malicious party may attempt to recover sensitive data from the deviceitself
2. may use the device to gain access to the organization's resources.

- Use of Untrusted Mobile Devices

In addition to company-issued and company-controlled mobile devices, virtually all employees will have personal smartphones and/or tablets. The organization must assumethat these devices are not trustworthy.

- Use of Untrusted Networks

If a mobile device is used on premises, it can connect to organization resources over the organization's own in-housewireless networks.

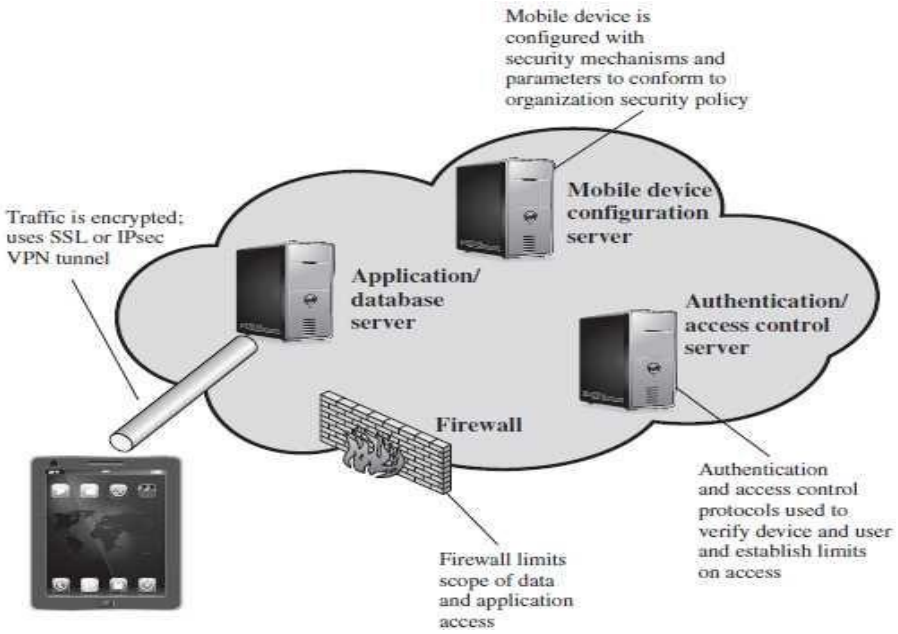
Thus, traffic that includes an off-premises segment is potentially susceptible to eavesdropping or man-in-the-middle types of attacks.

- Use of Applications Created by Unknown PartiesBy design, it is easy to find and install third-party

applications on mobile devices. This poses the obvious riskof installing malicious software.

- Interaction with Other Systems

Unless an organization has control of all the devices involvedin synchronization, there is considerable risk of the organization's data being stored in an unsecured location, plus the risk of the introduction of malware.



- **Use of Untrusted Content**

Mobile devices may access and use content that other computing devices do not encounter..

- Use of Location Services

The GPS service, it creates security risks. An attacker can use the location information to determine where the deviceand user are located, which may be of use to the attacker.

➢ Risk Model

cyber security risk modeling is the task of creating a variety of risk scenarios, assessing the severity of each, and quantifying the potential outcome if any scenario is realized – in a language that makes sense to your business.

Cyber risk modeling should not be confused with threat modeling. Threat model frameworks help identify cyber threats and vulnerabilities and inform and prioritize mitigation efforts. On the other hand, cyber risk modeling is an efficient and repeatable means of quantifying the likelihood of a cyber-attack. With this insight, your business can make robust decisions about where to focus investment for the greatest ROI.

An example of cyber security risk modeling

One of the most impactful examples of cyber security risk modeling is the quantification of cyber risk in financial terms as opposed to business terms. By establishing a universal understanding of cyber risk across your organization you can develop a more mature cybersecurity program and lead meaningful conversations on the business impact of different cyber scenarios and cybersecurity investments.

This analysis is not too different from the process of quantifying risk in a financial portfolio. For example, traders and portfolio managers use risk models to analyze and anticipate the impact of future events on performance so they can make preemptive decisions about where to invest funds.

A data-driven approach to understand risk exposure

Of course, any model is only as good as the data inputs and assumptions that go into it. The data must be current and accurately reflect the entire risk landscape. It's an overwhelming task for any security team. Digital ecosystems are expanding into the cloud and across business units and subsidiaries. It would take an army of resources to identify each digital asset, assess risk exposure, and calculate what a breach would mean financially.

The combined set of metrics delivers actionable analysis of cyber risk exposure across your business units, subsidiaries, and even M&A targets. And because no two risk scenarios are the same, you can simulate hundreds of thousands of events – ransomware, supply chain attacks, and more – and view the financial impact of each. You can also use these insights to diagnose the underlying vulnerabilities that impact financial exposure and inform what actions will deliver the greatest cyber risk reduction. Because risk is constantly evolving, the financial cyber risk quantification analysis is available on-demand and is easily repeatable so that you can measure risk exposure over time.

➢ Counter measure

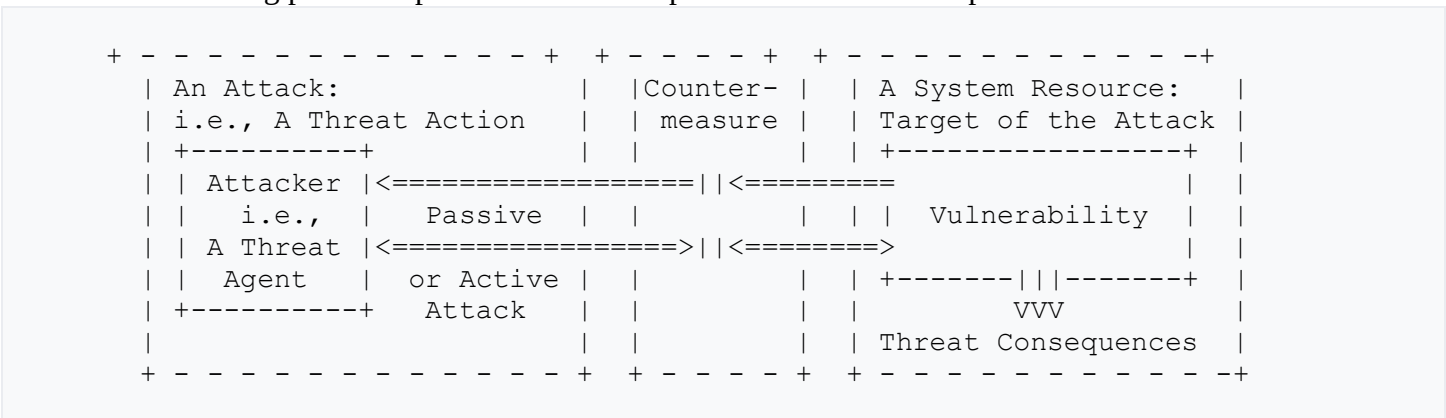
In computer security a **countermeasure** is an action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.

According to the Glossary meaning of countermeasure is:

The deployment of a set of security services to protect against a security threat.

A synonym is security control. In telecommunications, communication countermeasures are defined as security services as part of OSI Reference model

The following picture explain the relationships between these concepts and terms:



A resource (either physical or logical) can have one or more vulnerabilities that can be exploited by a threat agent in a threat action. The result can potentially compromises
the confidentiality, integrity or availability properties of resources (potentially different that the vulnerable one) of the organization and others involved parties (customers, suppliers).
The so-called CIA triad is the basis of information security.

The attack can be active when it attempts to alter system resources or affect their operation: so it compromises integrity or availability. A "passive attack" attempts to learn or make use of information from the system but does not affect system resources, compromising confidentiality.

A threat is a potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger enabling the exploitation of a vulnerability. A threat can be either "intentional" (i.e., intelligent; e.g., an individual cracker or a criminal organization) or "accidental" (e.g., the possibility of a computer malfunctioning, or the possibility of an "act of God" such as an earthquake, a fire, or a tornado).[1]

A set of policies concerned with information security management, the information security management systems (ISMS), has been developed to manage, according to risk management principles, the countermeasures in order to accomplish to a security strategy set up following rules and regulations applicable in a country

Electronic Destruction Devices

Devices such as a USB Killer may be used to damage or render completely unusable anything with a connection to the motherboard of a computer, such as a USB port, video port, Ethernet port, or serial port. Without proper protection, these devices may result in the destruction of ports, adapter cards, storage devices, RAM, motherboards, CPUs, or anything physically connected to the device attacked, such as monitors, flash drives, or wired switches. These types of devices can even be used to damage smartphones and cars, as well.

This threat can be mitigated by not installing or restricting physical access to easily accessible ports in situations where they are not necessary. A port-closing lock which permanently disables access to a port short of the actual port being disassembled. When it is necessary for a port to be accessible, an opto coupler can allow for a port to send and receive data to a computer or device without a direct electrical connection, preventing the computer or device from receiving any dangerous voltage from an external device.

Hard Drives and Storage

In an unsecured scenario, a malicious actor may steal or destroy storage devices such as hard drives or SSDs, resulting in the destruction or theft of valuable data.

If the data of a storage device is no longer necessary, data theft is best prevented against by physically destroying or shredding the storage device.

If the data of a storage device is in use and must be secured, one can use encryption to encrypt the contents of a storage device, or even encrypt the whole storage device save for the master boot record. The device can then be unlocked with a password, biometric authentication, a physical dongle, a network interchange, a one-time password, or any combination thereof. If this device is a boot drive, however, it must be unencrypted in a pre-boot environment so the operating system can be accessed. Striping, or breaking data into chunks stored upon multiple drives which must be assemble in order to access the data, is a possible solution to physical drive theft, provided that the drives are stored in multiple, individually secured locations, and are enough in number that no one drive can be used to piece together meaningful information.

Not to be neglected is the process of adding physical barriers to the storage devices themselves. Locked cases or physically hidden drives, with a limited number of personnel with knowledge and access to the keys or locations, may prove to be a good first line against physical theft.

What is Cloud Cryptography?

According to privacy experts, cryptography is the cornerstone of security. Cloud cryptography is the encryption of data stored in the cloud which adds a strong layer of protection and avoids a data breach. This practice safeguards data without delaying the data delivery. Cryptography expert Ralph Spencer Power said "information in motion and information at rest can be better protected by cryptography. Virtual data needs to be stored cryptographically by maintaining the control of the cryptographic key." Now, let us learn how to implement cryptography in the cloud and protect our cloud data.

How to Implement cryptography in Cloud Computing?

It's not possible to control cloud data physically. Cloud encryption is a way of protecting data and communication with the help of codes. Cloud data encryption can guard sensitive data and verify asset transfer without delaying the information transmission. Several tech giants like Google and Amazon define cryptographic protocols for their cloud computing to balance efficiency and security.

There are different kinds of cryptographic keys used by companies for **cloud security**. Cloud data encryption depends on three algorithms:

1. Symmetric-key
2. Asymmetric key
3. Hashing

Symmetric Algorithm

It utilizes one key for both encryption and information decoding. It doesn't need a lot of computational power and works extremely high in encryption. Symmetrical algorithms consist of two-way keys to guarantee verification and approval. Except if the client has the key, the encoded information is put away in the Cloud, and can't be decoded.

Some popular symmetric algorithms used in cloud computing algorithms are – Data encryption standard (DES), Blowfish, Advanced encryption standard, Triple DES, etc.

- **Advanced Encryption Standard (AES)** – It is used to encrypt digital data such as telecommunications, financial, and government. In AES, the same key is used for both encryption and decryption. It is a block of ciphertext that repeats itself after every defined step multiple times. It has a 128-bit block size, with key sizes of 128, 192, and 256 bits. It's efficient in both software and hardware.
- **Data Encryption Standard (DES)** – It adopts a 64-bit secret key, out of which 56 bits are created randomly and the remaining 8 bits are used for error detection. DES is implemented in hardware and is basically used for single-user encryption, for eg – files stored on a hard disk in encrypted form.

Asymmetric Algorithm

It utilizes different keys for encryption and decoding. Here, every beneficiary requires a decoding key. This key is referred to as the recipient's private key. Here, the encryption key belongs to a particular individual or entity. This sort of algorithm is considered the most secure as it requires both keys to get to a piece of explicit data.

- **Rivest Shamir Adleman Algorithm (RSA)** – It is one of the de-facto encryption standards and is used for a variety of platforms. It used different keys for encryption and decryption. The public key is known to everyone which can be decrypted using the private key only by the authorized person.
- **Elliptic Curve Cryptography (ECC)** – ECC is modern public-key cryptography that depends on number theory and mathematical elliptic curves to generate a short key. ECC is preferred by the security experts because of the small key size of the ECC.

Hashing

It is one of the major parts of block chain security. In the block chain, data is put away in blocks and interconnected with cryptographic standards like a string or chain. When an information block is added to

the chain, a particular code or hash is assigned to the particular block. Hashing is basically utilized for ordering and recovering things in a data set. It likewise utilizes two distinctive keys for encrypting and decoding a message. It likewise gives quicker information retrieval.

Advantages of cloud cryptography

- cryptography in the cloud is probably the most secure strategy to store and move the information as it complies with the limitations forced by associations like FIPS, FISMA, HIPAA, or PCI/DSS.
- The information stays private to the clients. cryptography in the cloud lessens the cybercrime cases.
- Companies get warnings promptly if an unauthorized individual attempts to access the data. The clients who have cryptographic keys are only allowed data admittance.
- The encryption keeps the information from being vulnerable when the information is being transferred from one PC then onto the next,
- Cloud encryption prepares organizations to stay proactive with all due respect against cyberattacks
- Receivers of the data can recognize if the information got is adulterated, allowing a prompt reaction and answer for the assault.

Disadvantages of cloud cryptography

- Cloud cryptography just grants restricted security to the information which is in transit.
- Cloud encryption needs exceptionally advanced systems to maintain encrypted information.
- The frameworks should be adequately versatile to update which adds to the involved costs.

Companies and organizations need to take a data-centric approach to protecting their sensitive information in order to guard against advanced threats in the complex and evolving environments of virtualization, cloud services, and mobility. Companies should implement data security solutions that provide consistent protection of sensitive data, including cloud data protection through encryption and cryptographic key management. A comprehensive platform for cloud security and encryption also should deliver robust access controls and key management capabilities that enable organizations to practically, cost effectively, and comprehensively leverage encryption to address security objectives.

6 Significant Cloud Security Threats

Organizations and businesses have had to turn to third-party cloud and managed security services to look for ways to bolster cybersecurity and shift from legacy to modern data platforms.

However, the sudden transition to the cloud has brought new security risks. This means that if your business or organization chooses to adopt cloud technologies and migrate your data over, you could be making a major mistake without being fully informed of the risks involved.

In this article, we will outline the six most significant cybersecurity threats for cloud networks that businesses face when migrating data or applications to the cloud. Take note that these cloud security threats are always evolving and the ones listed here are by no means exhaustive.

➢ Cloud Security Threats

Data Breaches

Data breaches occur when unauthorized individuals access cloud systems and interfere with the data stored in them. Whether attackers view, copy or transmit data, an organization's safety is not guaranteed once such individuals gain access.

Significant data breaches that have been costly to businesses include the mid-2018 Tesla cloud crypto-jacking that exposed sensitive telemetry data. This occurred due to the company's failure to encrypt one of its cloud accounts.

The primary cause of data breaches is human error. Lack of knowledge or not educating your staff on how to keep data safe and secure can easily expose your business to a hacker. This is why providing sufficient cybersecurity education on data protection to your employees is crucial, as nearly 90% of professionals agree that improved data protection skills can significantly reduce risks and data breaches happening within their respective organizations.

Insider Threats

Sometimes, the biggest threats to an organization's cybersecurity are internal. Insider threats are usually seen as more hazardous than outsider threats as they can take several months or years to identify.
The masterminds are usually individuals with legitimate access to an organization's cloud systems. Whether they happen intentionally or maliciously, insider threats will cause a lot of harm to your cloud system. Therefore, it is essential to detect, investigate and respond to them as fast as possible.

The reason why these attacks can go undetected for long periods is that businesses lack the proper systems to identify these attacks and are unprepared to identify and resolve them. In addition, companies have little to no control over underlying cloud infrastructure. Traditional security solutions may not be effective as long as significant power remains with the vendors.

Monitoring user analytics and gaining visibility into behavioral anomalies can be a way to signal an active insider threat as well as putting employees and processes to the test with adversary simulation and control tuning.

Denial-of-Service Attacks

Due to the rise of cyberattacks brought on by the global pandemic, an increasing number of companies are shifting their data control to the cloud. However, this leaves most applications and essential internal functions that are cloud-based exposed to denial-of-service attacks.
In a denial-of-service attack, a hacker floods a system with more web traffic than it can handle at its peak. This results in operations stalling entirely, with internal users and customers unable to access the system, making it unable to operate the business.

Subsequently, companies need to find ways to stop denial-of-service attacks before they occur and cause serious setbacks. One strategy is to rely on dynamic application security tools, which will scan your web applications for threats while they are running and can identify denial-of-service attacks in their early stages or before they happen.

Insecure Interfaces and APIs

Software user interfaces and APIs are usually responsible for the provision, monitoring and management of cloud services. Cloud service providers are working tirelessly to advance APIs and interfaces, but this growth has also increased security risks associated with them.

Cloud service providers use a specific framework to provide APIs to programmers, which leaves their systems more vulnerable to attackers. As such, organizations risk improper authorizations, previously used passwords and anonymous access. The best way to solve this is knowing how to properly design your cloud security with a multi-layer approach, which is required to help curb unauthorized access and ensure that the software you create is secure.

Hijacking of Accounts

The growing reliance on cloud-based infrastructure has also contributed to a high number of account hijacking cases. Depending on the attacker's intent and how they will use the accessed information, cloud account hijacking can have devastating consequences for a business, such as information being falsified or leaked to other parties.
Account hijacking attacks can also damage a brand's reputation and the relationships they have with their customers. The integrity and good reputation a company has built for years can be destroyed with one cyberattack. Legal implications could also follow if customers decide to sue the company for exposing their confidential data.

Having rock-solid facilities that utilize electronic surveillance and multifactor access systems is important to minimize the risk of hijacking and disruptions to operations. Having a provider that also offers features such as secure data transfer, encrypted data storage and security logs will provide detection of brute-force attacks.

Misconfigurations

Misconfigurations is one of the leading threats businesses face in their cloud-based systems. Most business owners are inexperienced in matters surrounding cloud-based infrastructure, which exposes them to various data breaches that can impact their operations.

Misconfigurations often results from the need to make cloud data accessible and shareable. Limiting access only to eligible people and, depending on the cloud service provider, can impact a company's ability to control these systems dramatically. Basic cloud storage services often come with critical security measures such as client-side encryption, intrusion detection systems and internal firewalls. Being familiar with vendor-provided security settings is critical

➢ Security at service layers

When some enterprises migrate to the cloud, they wrongly assume that workload security is now in the hands of their cloud provider.

In reality, most cloud vendors enforce what's called a shared responsibility model. This model varies depending on the cloud computing service category -- SaaS, PaaS or IaaS -- but, in all cases, security responsibilities are split to some degree between the cloud provider and its users.

When applications and servers are hosted in-house, IT operations admins' security responsibilities are clearly defined; teams can physically see, or at least have direct control over, the IT resources that run in their data center. With cloud computing, however -- where users essentially "rent" compute resources from a provider admins must drastically change how they manage workloads. And, in some cases, this creates gaps in security coverage.

While SaaS and PaaS each present unique cloud security considerations, admins can also apply some key best practices from their days of securing on-premises resources.

SaaS security emphasizes access control

With SaaS, enterprises access an application that is fully hosted and managed by a cloud provider. It might appear as if IT teams are free from any security responsibilities, particularly when compared to how they maintain on-premises workloads. The problem, however, is that this is an apples-to-oranges comparison. IT teams still need to manage configurations and access controls for SaaS applications.

The SaaS provider does manage and secure the infrastructure, OS and application stack -- but IT teams still need to manage configurations and access controls for SaaS applications. Most SaaS offerings -- whether Microsoft Office 365 or a learning management system or HR tool -- come with admin accounts, from which IT staff can add or remove user access permissions for the application. Admins also can enable or disable certain application features to fit the enterprise's needs and compliance model. Limit access to these administrative accounts to only a select group of operations admins, and where possible, make the admin accounts separate from their daily user accounts to avoid accidental SaaS-wide changes.

A cloud migration is a complex process, during which IT teams might grant permissions on a temporary basis -- and they can forget to reset access after the migration is complete. Account auditing is an essential cloud security consideration for all applications hosted there.

PaaS security brings greater responsibility

Compared to SaaS, IT staff's responsibilities increase with PaaS deployments. PaaS grants admins more control over the application stack -- which shifts more security responsibilities from the cloud provider to the user.

PaaS security can be a challenge, organizationally, for operations staff, since the team that owns the application typically handles application security, rather than the security and infrastructure team. In other words, PaaS puts a lot of security responsibility onto people whose primary concern is application delivery.

Enterprises have more security responsibilities for PaaS than they do with SaaS.

This gap between the application owner and the security teams has always existed, but it becomes more evident with cloud adoption. Ops teams may find they have another hat to wear; while they won't be responsible for securing the cloud application itself, they will have to enforce -- and verify -- that other parties follow security best practices.

A change to toolsets -- and processes

Another cloud security consideration is that ops and the security teams can't use traditional tools and processes for cloud security testing and verification. For example, in some cases, enterprise IT teams must notify their cloud provider when they plan to run security scans or penetration tests on that provider's

resources. Even if a cloud provider does not require these notifications, it generally defines certain practices that users must follow to perform these tests. In addition, a cloud provider's internal security teams have the right to respond to tests performed on the platform.
Cloud providers' native tools, such as AWS Security Hub and Azure Security Center, along with several third-party products, such as HyTrust and CipherCloud, can validate cloud deployment security. Cloud providers don't want to see their users experience a security issue -- because it's simply bad for business -- so take advantage of the tools they offer.
Overall, though, cloud security considerations are less about technical shortcomings, and more about processes and verification. IT ops teams need to emphasize policy and procedure -- this will go much further to secure a cloud deployment than any one tool can.

➢ Introduction to Block chain

Think of a block chain as a novel, digital form of record-keeping.
Blockchain is the underlying technology that many cryptocurrencies — like Bitcoin and Ethereum — operate on, but its unique way of securely recording and transferring information has broader applications outside of cryptocurrency.
A block chain is a type of distributed ledger. Distributed ledger technology (DLT) allows record keeping across multiple computers, known as "nodes." Any user of the block chain can be a node, but it takes a lot of computer power to operate. Nodes verify, approve, and store data within the ledger. This is different from traditional record-keeping methods which store data in a central place, such as a computer server.
A block chain organizes information added to the ledger into blocks, or groups of data. Each block can only hold a certain amount of information, so new blocks are continually added to the ledger, forming a chain.
Each block has its own unique identifier, a cryptographic "hash." The hash not only protects the information within the block from anyone without the required code, but also protects the block's place along the chain by identifying the block that came before it.

Once information is added to the block chain and encrypted with a hash, it's permanent and unchangeable. Each node has its own record of the full timeline of data along the block chain, going back to its start. If someone tampered with or hacked into one computer and manipulated the data for their own gain, it wouldn't alter the information stored by other nodes. The altered record can be easily distinguished and corrected, since it doesn't match the majority.

"The way that the system works, it's almost impossible for someone to replicate the computing power that happens on the back end to reverse engineer it, and somehow figure out what all those hashes are," Agarwal says.

How it Works

Here's an example of how block chain is used to verify and record Bitcoin transactions.

- A consumer buys Bitcoin.
- The transaction data is sent across Bitcoin's decentralized network of nodes.
- Nodes validate the transaction.
- After approval, the transaction is grouped with other transactions to form a block, which is added to an ever-growing chain of transactions.
- The completed block is encrypted, and the transaction record is permanent; it cannot be removed or altered on the block chain.

Bitcoin's block chain is public, which means anyone who owns Bitcoin can view the transaction record. While it can be difficult to trace the identity behind an account, the record shows which accounts are transacting on the block chain. Public block chains also allow any user with the required computer power to participate in approving and recording transactions onto the block chain as a node.
But not all block chains are public. Block chains can be designed as private ledgers, so an owner is able to limit who can make changes or additions to the block chain. While the pool of participants may be smaller

on a private block chain, it's still decentralized among those who participate. Private block chains maintain the security of any data stored within the database using the same encryption methods.
The idea of a secure, decentralized permanent record of information has drawn interest across a number of industries, and potentially holds solutions for many security concerns, record-keeping processes, and data ownership issues we face today.

Innovative applications of blockchain

You don't need to look far to come up with a list of innovative ways in which blockchain technology is being applied. A wide range of fields, including healthcare, real estate, government, and music are finding a use for blockchain's powerful, secure way of storing, verifying, and encrypting data.8 Here are seven more applications of blockchain technology, some of which are underscored by cryptocurrencies:

Finance

One of the main services of the financial sector is to store money and transfer it from one entity to another. This requires a trustworthy intermediary, in the form of a bank. Blockchain is now effectively eliminating the need for such intermediaries by decentralizing transactions. By moving the means of transaction out of siloed, closed networks, blockchain is helping to solve some of the challenges around the interoperability of disparate financial systems around the world.9.The ability to track all transactions increases the transparency and security of blockchain-based payments too. This is beneficial both to the parties of a transaction and to relevant regulators.10

Smart contracts

Smart contracts act as self-executing programs, triggered automatically when predetermined conditions are met, that facilitate the terms of agreement between the seller and buyer directly. As they are executed on a blockchain network, the transactions are trackable, transparent, and irreversible.This type of automation can significantly boost productivity while slashing costs in business. Put simply, it helps you exchange property, shares, legal documents, or anything of value in a manner that's transparent and free of conflict, while also avoiding the expense of a middleman.[12]

Cybersecurity

Data stored on blockchain is rendered tamper-proof because the network of nodes (the disparate computers on which the shared database is stored, and which validate transactions) can cross-reference to locate the source of a disputed change, so the technology has a number of potential cybersecurity applications. Storing information across a network of devices reduces the risk of a hacker exploiting a single point of vulnerability. Similarly, decentralizing control of edge devices (which provide an entry point into enterprise or service provider core networks) and Internet of Things devices can render these devices more secure against attacks.

Health records

A decentralized, secure, trustworthy blockchain system has clear applications for the storage of healthcare records. Personal health records (PHR) collect data from sources including medical centers, devices, clinics, and pharmacies, and are primarily managed by patients. Electronic health records (EHR) are digital records of patients' medical history, and are managed by doctors.
As patients manage PHRs, the validity of that information is sometimes doubted. Storing them on block chains would ensure they are traceable, transparent, unchangeable, auditable, and secure.
EHRs, on the other hand, are typically stored in centralized legacy systems, which may not be interoperable between different healthcare facilities. Blockchain could offer a solution, with EHRs stored securely on a decentralized system that can be accessed – by both patients and healthcare workers – across systems and organizations.

Non-fungible tokens

NFTs, as they're more commonly known, are tokens on block chains, but they differ from cryptocurrencies in that they are unique digital assets.16 Technically, NFTs can represent ownership of anything, but they are mostly used to buy and sell digital art. In many cases, this digital art already exists

and is freely available on the internet for anyone to view, buy, or download. What an NFT confers is ownership of that art. Think of it as the difference between owning an original painting and a print of it.17
Voting

Recording and storing high-value, high-volume pieces of data is inherent to the voting process. This makes blockchain an ideal technology for updating the voting system. Because all nodes on a blockchain must verify any information entered onto it, people could potentially cast their votes online without fear of fraud. It also creates greater certainty for electoral officials, who can tally votes certain in the knowledge that each is attributable to only one individual.

- A **cryptocurrency**, **crypto-currency**, or **crypto** is a digital currency designed to work as a medium of exchange through a computer network that is not reliant on any central authority, such as a government or bank, to uphold or maintain it.

Individual coin ownership records are stored in a digital ledger, which is a computerized database using strong cryptography to secure transaction records, to control the creation of additional coins, and to verify the transfer of coin ownership. Despite their name, cryptocurrencies are not necessarily considered to be currencies in the traditional sense and while varying categorical treatments have been applied to them, including classification as commodities, securities, as well as currencies, cryptocurrencies are generally viewed as a distinct asset class in practice. Some crypto schemes use validators to maintain the cryptocurrency. In a proof-of-stake model, owners put up their tokens as collateral. In return, they get authority over the token in proportion to the amount they stake. Generally, these token stakers get additional ownership in the token over time via network fees, newly minted tokens or other such reward mechanisms.

Cryptocurrency does not exist in physical form (like paper money) and is typically not issued by a central authority. Cryptocurrencies typically use decentralized control as opposed to a central bank digital currency (CBDC). When a cryptocurrency is minted or created prior to issuance or issued by a single issuer, it is generally considered centralized. When implemented with decentralized control, each cryptocurrency works through distributed ledger technology, typically a blockchain that serves as a public financial transaction database.

A cryptocurrency is a tradable digital asset or digital form of money, built on blockchain technology that only exists online. Cryptocurrencies use encryption to authenticate and protect transactions, hence their name. There are currently over a thousand different cryptocurrencies in the world.

Bitcoin, first released as open-source software in 2009, is the first decentralized cryptocurrency. Since the release of bitcoin, many other cryptocurrencies have been created.

BitCoinSecurity and Working

Bitcoin, often described as a cryptocurrency, a virtual currency or a digital currency - is a type of money that is completely virtual.
It's like an online version of cash. You can use it to buy products and services, but not many shops accept Bitcoin yet and some countries have banned it altogether.
However, some companies are beginning to buy into its growing influence.
Bitcoin is a type of digital token that can be sent electronically through a decentralized digital payment network. Bitcoins can be sent from person to person, anywhere in the world; indeed, Bitcoin was initially intended to be used as a secure electronic cash and payment system.
Bitcoin is built on blockchain technology. A blockchain is a type of digital ledger that records information (such as transactions) in a way that makes it nearly impossible to edit or alter that information. This way of recording information is inherently secure, but Bitcoin takes it a step further by specifically employing *a* decentralized blockchain, which depends on a peer-to-peer network to verify transactions.

How does Bitcoin work?

Each Bitcoin is basically a computer file which is stored in a 'digital wallet' app on a smartphone or computer.
People can send Bitcoins (or part of one) to your digital wallet, and you can send Bitcoins to other people.
Every single transaction is recorded in a public list called the blockchain.
Bitcoin mining is the process by which Bitcoin transactions are validated. It's *also* the process by which new Bitcoins enter circulation. Allow us to explain.
We just mentioned that Bitcoin's consensus model requires a ton of computing power to function. This consensus model is called "proof-of-work," and it's integral to an understanding not only of how Bitcoin transactions are verified, but also of how new Bitcoins are created.
Bitcoin's "proof-of-work" model requires miners on the Bitcoin network to solve highly complex math problems to validate transactions. In return, these miners are rewarded with newly created Bitcoins. The fact that so many computers are spending so much power to validate transactions means that it's essentially impossible to get at least 51% of those computers to validate an inaccurate version of the ledger.

What are Bitcoins used for?

Though it was originally conceived of as a cash payment system, Bitcoin has grown into a number of different uses. Here are a few:

- You can use Bitcoin to buy things. From glamorous luxury cars to everyday insurance, you can use Bitcoin to buy all kinds of things. And with Bitcoin debit cards, which are loaded with cryptocurrency but are also capable of completing day-to-day transactions in fiat currency, you can "use" Bitcoin anywhere that accepts plastic.
- You can consider Bitcoin as a store of value. Though it's a far cry from typical investments, Bitcoin is also considered by many as an appealing store of value. Its volatile, whiplash pricing means that Bitcoin is a highly risky asset, but that hasn't stopped many speculators from piling in. The total number of Bitcoins is capped, which encourages some to see it as "digital gold."
- You can buy, sell, and trade Bitcoin. Due to their volatile and unpredictable pricing on the open market, Bitcoin and other cryptocurrencies have become popular with day traders and investors alike. Keep in mind, though, that any investment in cryptocurrency carries with it serious risks.

Advantages of Bitcoin

- Bitcoin is by its very nature secure, with little risk of false or double-spending transactions being verified by the network.
- Bitcoin is a highly transparent financial vehicle, with every transaction recorded in the blockchain for all to see.
- Bitcoin offers potential for major returns thanks to its high price volatility—though this also comes with significant risk

Disadvantages of Bitcoin

- Bitcoin's volatility can also be seen as one of its chief disadvantages, especially if you plan to use it as a store of value.
- Bitcoin isn't yet ready to replace cash for day-to-day needs.
- Bitcoin mining is an energy-intensive process that requires expensive equipment. This makes Bitcoin less appealing to environmentalists and those concerned about climate change.

➢ Ethereum

Ethereum isa decentralized, open-source blockchain with smart contract functionality. **Ether** (**ETH** or **Ξ**) is the native cryptocurrency of the platform. Among cryptocurrencies, Ether is second only to Bitcoin in market capitalization.

Ethereum allows anyone to deploy permanent and immutable decentralized applications onto it, with which users can interact. Decentralized finance (DeFi) applications provide a broad array of financial services without the need for typical financial intermediaries like brokerages, exchanges, or banks, such as allowing cryptocurrency users to borrow against their holdings or lend them out for interest. Ethereum also allows users to create and exchange NFTs, which are non-interchangeable tokens connected to digital

works of art or other real-world items and exchanged as a variety of digital property. Additionally, many other cryptocurrencies operate as ERC-20 tokens on top of the Ethereum blockchain and have utilized the platform for initial coin offerings.

Ethereum is permissionless non-hierarchical network of computers (nodes) that build and come to a consensus on an ever-growing series of "blocks", or batches of transactions, known as the blockchain. Each block contains an identifier of the chain that must precede it if the block is to be considered valid. Whenever a node adds a block to its chain, it executes the transactions therein order, thereby altering the ETH balances and other storage values of Ethereum accounts. These balances and values, collectively known as the "state", are maintained on the node separately from the block chain,

Each node communicates with a relatively small subset of the network—its "peers". Whenever a node wishes to include a new transaction in the blockchain, it sends the transaction to its peers, who then send it to their peers, and so on. In this way, it propagates throughout the network. Certain nodes, called miners, maintain a list of all of these new transactions and use them to create new blocks, which they then send to the rest of the network. Whenever a node receives a block, it checks the validity of the block and of all of the transactions therein and, if it finds the block to be valid, adds it to its blockchain and executes all of those transactions. Since block creation and broadcasting are permissionless, a node may receive multiple blocks competing to be the successor to a particular block. The node keeps track of all of the valid chains that result from this and regularly drops the shortest one: According to the Ethereum protocol, the longest of multiple competing chains is to be considered the canonical one.

Ether

Ether (ETH) is the cryptocurrency generated by the Ethereum protocol as a reward to miners in a proof-of-work system for adding blocks to the blockchain. It is the only currency accepted to pay for transaction fees, which also go to miners. The block-addition reward together with the transaction fees provides the incentive to miners to keep the blockchain growing (i.e. to keep processing new transactions). Therefore, ETH is fundamental to the operation of the network. Each Ethereum account has an ETH balance and may send ETH to any other account. The smallest subunit of ETH is known as a Wei, named after cryptocurrency.

Accounts

There are two types of accounts on Ethereum: user accounts (also known as externally-owned accounts) and contracts. Both types have an ETH balance, may send ETH to any account, may call any public function of a contract or create a new contract, and are identified on the blockchain and in the state by an account address.

User accounts are the only type of account that may create transactions. For a transaction to be valid, it must be signed using the sending account's private key, the 64-character hexadecimal string from which the account's address is derived. The algorithm used to produce the signature is ECDSA. Importantly, this algorithm allows one to derive the signer's address from the signature without knowing the private key.

Contracts are the only type of account that have associated code (a set of functions and variable declarations) and contract storage (the values of the variables at any given time). A contract function may take arguments and may have return values. Within the body of a function, in addition to control flow statements, a contract's code may include instructions to send ETH, read from and write to its storage, create temporary storage (memory) that vanishes at the end of the function, perform arithmetic and hashing operations, call its own functions, call public functions of other contracts, create new contracts, and query information about the current transaction or the blockchain.

➢ Ecosystem

What is a blockchain ecosystem?

A blockchain ecosystem is a group of various technological elements capable of interacting to create a system that performs a specified function. This system encompasses multiple governing structures like individual participation, data ownership, funding, exit and entrance criteria, information shared with the system's participants.

The blockchain ecosystem can provide true decentralisation, immutability, transparency, accountability and flexibility to day-to-day operations.

These advantages can be a boon for technology startups and projects as it creates an interconnected network, even if they must consider what information they want to share within the network.

The types of blockchain ecosystems

A blockchain ecosystem could have participants in its network with different goals and business models. They can even have distinct contributions to the network. In fact, the various participants can even be competitors. In a blockchain ecosystem, every participant would be looking out for themselves and what business value they receive as a part of the ecosystem.

The type of blockchain ecosystem for a shared blockchain project will depend on the participants in the network. That is why different types of blockchain ecosystems accommodate the specific needs of the participants in the network. Here are some of the notable ones being used these days.

Single party-led: A Single party blockchain project is led by a single organisation where its stakeholders have a mutual benefit for participating in the network. An example of this ecosystem would be Bumble Bee Foods. They created an ecosystem of various stakeholders to improve the traceability of yellowfin tuna fish from the ocean to a customer's dinner table.

The stakeholder of Bumble bee Foods includes fishermen, packagers, transportation personnel, distributors, and retailers who record the fish's details on the blockchain. Customers can use a QR code to view this information. It can help improve the buyer's confidence in the fish's freshness.

Joint venture ecosystem: Joint ventures ecosystems usually have two or more organisations at the helm. These ecosystems are slowly becoming popular and are now overtaking formal joint ventures. These ecosystems are created to pool sources for a common goal.

The only question in the ecosystem is whether the organisations forming a strategic business association are a new legal entity or just entering a formal contractual arrangement.

An example of a joint venture ecosystem is BunkerTrace, an association between Forecast Technology Ltd. and BLOC (Blockchain Labs for Open Collaboration). BunkerTrace is a marine fuel tracking solution.

Regulatory blockchain ecosystems: This ecosystem comprises various government agencies that share a project and have to self-report for compliance. An example of a regulatory ecosystem would be the shared project between Marine Transport International and the Recycling Association. They use a blockchain-based tool to capture data concerning shipments of recyclable waste from Britain.

A crucial aspect of all these ecosystems is how they will be funded. Typically, ecosystems are excluded from the day-to-day business model funding. An organisation has to set aside a budget for creating a blockchain ecosystem as they have to consider various governance and operations costs for the ecosystem.

The rapid growth of the crypto ecosystem presents new opportunities. Technological innovation is ushering in a new era that makes payments and other financial services cheaper, faster, more accessible, and allows them to flow across borders swiftly. Crypto asset technologies have potential as a tool for faster and cheaper cross-border payments. Bank deposits can be transformed to stable coins that allow instant access to a vast array of financial products from digital platforms and allow instant currency conversion. Decentralized finance could become a platform for more innovative, inclusive, and transparent financial services. Despite potential gains, the rapid growth and increasing adoption12 of crypto assets also pose financial stability challenges. This chapter discusses the implications of the expansion of the crypto ecosystem and provides an assessment of their associated financial stability risks. For emerging market and developing economies, greater use of crypto assets presents some benefits, but

also macro-financial risks, especially with respect to asset and currency substitution—referred to in this chapter as cryptoization.

➢ Service Risk

Mobile Risks and Attacks Mobile applications are implemented in many of the same languages as their desktop and Web counterparts (e.g., Objective-C and Swift for iOS, Java for Android), and therefore are susceptible to many of the same vulnerabilities and attacks associated with those languages including infection and compromise by malicious software including spyware, Trojan horse programs, worms, and computer viruses. Phishing and other social engineering tactics prey on the weaknesses of the users. Other attacks target the mobile application itself, the server to which the mobile application speaks, unprotected internal APIs, alternate routes through and around security checks, and open server ports.

As with any technology channel, there are risks and threats associated with the mobile platform. It is possible for organizations to mitigate the potential risks and vulnerabilities during the development of mobile applications by establishing (or optimizing) formal security policies, procedures, and standards; education and training; and security engineering activities. These strategies are discussed in more detail in Mobile Risk and Threats – Part Two: Implementing Countermeasures.

MOBILE-SPECIFIC CHALLENGES

Due to the nature of how mobile devices function, they tend to have unique vulnerabilities when compared to desktops and servers, each with its own idiosyncrasies, built-in defenses, attack vectors, and threats. For example:

- **Physical Size** – The small size of mobile devices enables their distinctive portability – but makes them more susceptible to being lost, stolen, or temporarily misplaced. Once a mobile device is out of the authorized user's hands the device's stored user credentials, personal and corporate data, and gateway applications (such as VPN) for authorized access to corporate systems are at risk. In addition, the smaller screens and keyboards of mobile devices often force developers to make security trade-offs to accommodate a better mobile user experience.

- **Mobile Connections** – Mobile devices connect through a variety of networks to access, receive, or transmit data – sensitive or otherwise. Networks include GSM, 3G, and 4G; Bluetooth, 802.11-based wireless networks, and SMS and MMS texts. Each has its own security strengths and limitations, and each is a vector for remote exploits including data leakage or interception by malicious users – particularly if the mobile user isn't aware of the dangers or vulnerabilities.

- **Data Privacy and Security Concerns** – Mobile applications can take advantage of mobile-specific capabilities such as precise and continuous device location information (a weather app that uses device location to display local weather), physical sensor data (Touch ID), personal health metrics (Fitbit), and photos and audio about the device's user. The data collected by, stored in, and often transmitted by these mobile applications, though, raises privacy and security concerns if that information is exposed via these applications to unauthorized users.

➢ App Risks

Attackers can potentially use many different paths through your application to do harm to your business or organization. Each of these paths represents a risk that may, or may not, be serious enough to warrant attention. Sometimes these paths are trivial to find and exploit, and sometimes they are extremely difficult. Similarly, the harm that is caused may be of no consequence, or it may put you out of business. To determine the risk to your organization, you can evaluate the likelihood associated with each threat agent, attack vector, and security weakness and combine it with an estimate of the technical and business impact to your organization. Together, these factors determine your overall risk.

Risks.

Each organization is unique, and so are the threat actors for that organization, their goals, and the impact of any breach. If a public interest organization uses a content management system (CMS) for public information and a health system uses that same exact CMS for sensitive health records, the threat actors and business impacts can be very different for the same software. It is critical to understand the risk to your organization based on applicable threat agents and business impacts. Where possible, the names of the risks in the Top 10 are aligned with Common Weakness Enumeration (CWE) weaknesses to promote generally accepted naming conventions and to reduce confusion