What is an electron cloud theory

The opinions expressed by the participants of the entrepreneurs are their own. With more sensitive data stored in the cloud than ever before, entrepreneurs need to know how to keep information about their companies and their customers safe. Cloud service providers can successfully protect data physically and technologically while in the cloud, but that information can be vulnerable to hacking once it leaves the cloud to interact with another system. Even when companies are fully cloud-based, they often use backup data and in-place storage in some way. These systems also fall under your responsibility. Just look at the February StreetEasy breach, in which hackers stole information from a million accounts. Hackers did not gain access to this information during the day-to-day activities of the real estate company; they stole it using a backup database from 2016. Personal information from these accounts, including email addresses, usernames, the last four credit card numbers, expiration date and more, is now available for sale on the dark web. This lesson is difficult (and costly) for entrepreneurs: You have to protect data every step of the way. Related: 7 Amazing Places Hackers HideIronically, the myriad benefits of cloud storage can become a risk if businesses are not careful. Transactional data requests can be made and made from almost anywhere in the world, using any connected device - when the doctor's office requests access to patient hospital records, for example, or when a customer buys shoes online. This fast connection makes business operations smoother, faster, and much more efficient. This also means that the data can be left open if you do not take appropriate precautions. To protect your data with each transaction, take the following steps: 1. The practice of Internet security. Using virtual private networks (VPNs) and outlet/transport layer security (SSL/TLS) helps ensure that your Internet connection doesn't leave you open when dealing with data that moves from one system to another. A VPN makes your connection private and keeps your online activity, IP address and device information anonymous. Use a VPN to remotely access computers or networks, especially if you or your employees use public Wi-Fi.SSL/TLS to encrypt and protect sensitive data when it is transferred between two systems (such as a client/server or basket/browser), preventing this information from being read and altered. When you access the website to make a purchase, make sure the address starts at https, which checks that the site encrypts and hides your data from Eye. Related: 12 simple things you can do to be safer Online2. Encryption of connected devices. Encryption processes must go beyond information stored in the cloud, cloud, with so many connected and external devices used in conventional business operations. As a business owner, you need to make sure that you encrypt any connected devices, hard drives, USB drives and related devices. Any unencrypted data stored on these devices jeopardizes the privacy, finances and identity of your company and your customers. Some of the largest international data breaches in history have been tracked back into infected USB drives, including a U.S. Department of Defense breach in 2008. For example, we had a health care client who is legally required to protect any device that may contain patient health information (PHI). Unfortunately, someone stole an unencrypted doctor's laptop that contained patient records from his car during lunchtime, leading to a violation that incurred a huge fine (HIPAA violations can range from $100 to $1.5 million). Unencrypted data is like transferring your wallet to a stranger, including credit cards, insurance cards and forms of identification. By encrypting your devices, you ensure that people are unable to obtain sensitive data from a stolen or lost hard drive without an encryption key3. Several factors are better than one. What training does your company currently provide to employees to create, store, and protect their passwords? How does your company offer password-protected customer accounts? The reality is that most passwords are not secure - easy to remember usually means easy to crack. Businesses should use multi-factor authentication (MFA) as a baseline. The principle behind the MFA is that no authentication factor is perfect. The second or third factor can compensate for the weaknesses of others. Complete your password with one or two authentication factors that other people find easy to guess, such as using an authentic on a mobile device or biometric factor such as a fingerprint or voice. Related: What you need to know about multifactor Authentication4. Protect backups in the face of ransomware. When ransomware attacks the machine, backups are usually the last line of defense. That's why today's attackers use more sophisticated programs to infiltrate warranties. In March 2018, the world of cybersecurity was introduced into a ransomware program that not only encrypts files, but also intentionally removes backups until the victim fulfills the hacker's demands. Malwarebytes' 2017 report showed that ransomware detection grew by 90 percent and 93 percent for businesses and consumers, respectively, and that these attacks are becoming more common. Always protect your hardware and software using antivirus and antivirus applications, or you'll be an easy target. With the number of connected devices, data transfers, and backups required to perform typical business operations, companies must protect data every step of the way. Even in cloud storage or cloud computing data can be vulnerable when it's on the go, in backups, or stored on unencrypted devices. Take these steps to protect your data and your customers' information. istockphoto s. What is a cloud, exactly? First: Files don't literally shine into the sky. Cloud computing refers to a method - via the Internet - by which files are transferred from a computer (or smartphone or tablet) to physical servers. For example, Gmail messages are stored on Google servers (webmail is a form of cloud computing), so you can check your email from anywhere. Similarly, if you save or back-up files, such as music or photos, using a cloud service (see below for our samples), you can get them on almost any Internet-enabled device. If I hit my files on someone else's property, how can I know they're safe? Reputable companies store files on more than one server, in more than one center, so even if one fails, it's backed up. There may be failures in which the service may be temporarily slow or unavailable. (Last year, Amazon had two briefs that affected some of the cloud services it hosts, such as Foursquare.) But you can always save important files on your computer or external drive as another backup form. From a privacy standpoint, a good service uses safeguards such as password, SSL encryption to transfer files, and encrypted file storage, so personal information is unlikely to be hacked. The service should also assure you that the physical locations of servers are protected by both security staff and technologies such as fingerprint scanners, allowing only authorized access. What else can you do with cloud computing? It's not just about backing up. Many cloud computing services also have file-sharing capabilities. This means that you can save files for your account (such as a photo folder) and then give others access to view or edit them - great if, for example, you're trying to put all family vacation photos in one place. You can also share between devices (thus solving the problem of how to get photos from your mobile phone, for example). OUR RECOMMENDATIONS EASY TO USE dropbox.com - As the name suggests, just drag and drop any files you want to keep in the service. To get them, sign up for an account from any Internet-enabled device or email a file-sharing link. One drawback: This is not the best option to back up all the files because they have to be dropped manually. First 2 Free It's $10 a month for 50GB or $20 for 100GB. Full-FEATURED sugarsync.com - After setting up, it shares files among almost any group of Internet-enabled devices (computer, smartphone, tablet). The computer can be installed to automatically back up. You can also edit files offline. they sync the next time you connect. Its large mobile apps provide easy access to files on the go. The 5GB plan is free; other plans have free trials and start at $5 per month (or $50 per year) for 30GB or up to $80 per month (or $800 per year) for 1TB. This content is created and supported by a third party and is imported to this page to help users provide their email addresses. You can find more information about this and similar content in piano.io Cloud File Storage in the cloud (online). Instead of storing files on your local hard drive, external hard drive, or flash drive, you can save them online. There are several reasons for using cloud storage services. Maybe your local hard drives don't work on drive space, in which case you can use the cloud as extra storage. If you want to be able to transfer your music collection from anywhere, access your work files at home, easily share vacation videos, etc., you can upload files online to the cloud storage service. Another reason to use cloud storage is that you want to keep important files safe with your password and encryption. In short, cloud storage is useful not only when backing up, but also for security and the ability to easily share files with others or access them yourself from anywhere in the world: your phone, tablet, or other computer. Thomas Kuhlenbeck/ Getty Images When you upload a file to the Internet and this file exists for a long period of time, it is considered a cloud storage. The simplest type of cloud storage loads something onto the server and has the ability to get it again if you want. The reputable cloud storage service protects the files behind encryption and requires you to enter a password to have access to the files. In most cases, a cloud storage account can be protected by two-factor authentication, so anyone who wants to access your files should know not only the password, but also another code sent to your phone on requesting login. Most cloud storage services allow you to download all types of files: videos, photos, documents, music, or anything else. However, some are limited to accepting only certain types of files, such as only images or music. Cloud storage services tend to be pretty clear about what is allowed and what is not. Different cloud storage services allow you to upload files to an online account in a variety of ways. Some support in the browser only downloads, which means you have to log on to the cloud storage service's website to download your data, but most are desktop apps that make downloading files easier to simply drag and drop into a dedicated Service. Most of them also support uploading images and videos from your phone. Less common torrent cloud storage services, which are online torrent customers, which not only allow you to download torrents from your browser, but also store files in your online account for streaming or downloading later. Once your files are stored online, depending on how the service works, the service, you get can include the ability to stream video and music, access files from your mobile device, easily share files with others through a special sharing link, download files back to your computer, delete them to make room in your account, encrypt them so that even the service can't see them, and more. Cloud storage and cloud backup are easily confused. Both work the same way and have a similar end result: files are stored on the Internet. But there are two completely different reasons to use these services, and knowing how important they are, so you know which one to choose for your own situation. Cloud storage is a selective backup procedure whereby you choose which files to store online and then send them to your online account. When you delete a file on your computer, back up the web, the file is still in your cloud storage account because it's not actually tied to your computer anymore; it's just one file that you've uploaded online. Cloud backup is when you install a program on your computer and tell it to back up certain files online. Step beyond cloud storage, the backup service will also download any changes made to the file so that the current version is always stored online. In other words, if you delete a file from your computer, it can also be removed from your online backup account, and if you change the file on your computer, the online version will change too. The backup service is great if you want to always keep a huge number of files back up online. In case your computer suddenly stops working, you can recover all these files on a new computer or on another hard drive and you will get the same copies that you had the last time the backup program stored those files online. Cloud storage is less practical as a permanent backup solution and more useful as a way to back up certain files you want to access from anywhere in the world or share with others. The versions of files in your cloud storage account are the same as the versions you downloaded, regardless of whether you changed them on your computer. Like backing up online, you can still download files again if you need to, for example, if your computer falls. While there are many cloud storage providers, some of the most familiar ones are listed below. Amazon Drive offers 5GB of free cloud storage. If you have an Amazon Prime account, the free plan includes Unlimited photo storage and 5GB for other file types. You can pay more if you need extra space. Google Drive is a cloud storage built to keep Google products running smoothly. You get 15GB of free online storage with Google Drive to store documents, photos, music and videos. You can go to Google One for more space, somewhere from 100GB to 30TB. Microsoft OneDrive is a version of Microsoft's cloud storage. Users get 5GB of free space for any type of file, and Google Drive, OneDrive works seamlessly with Microsoft products such as Outlook Mail.Apple iCloud is Apple's cloud storage service that is available to any Apple user, whether you have a Mac, iPhone, iPad or iPod touch. You can get 5GB for free, but you can buy more. Much like an online backup service, iCloud can be used to automatically back up phone images, email and more. Dropbox provides its users with 2GB for free and allows you to access files from the Internet, desktop or mobile device. Dropbox Plus or Professional can be purchased for 1TB or more online storage space. There are also Dropbox business plans. Numerous cloud storage providers out there would like to see your business, so this can be misleading knowing which one to choose. Consider a few factors before choosing any online cloud backup service. Security: Your data must be encrypted to keep it a secret. If you are concerned that the service itself may open the files and see all your data backup, go with a service that has zero knowledge of encryption. Price: The cost is determined by how much space you expect to need. Many services offer either a trial period or free storage to allow you to try out your features. Similarly, go with a service that can accept the types of files you want to store online, such as a music storage service, if you store music online. Features: Knowing what features your cloud storage service supports is important when choosing the right one for you. Comparing the best free cloud storage services can help you identify between a few of the best. Aside from that, do some research on the company's websites to see what they offer, such as if they support streaming media files from their website or mobile app if that's what you need. Easy to use: Downloading and accessing files in the cloud should be clear and easy to understand. If you want to be able to do this with your desktop, make sure it's simple and won't leave you scratching your head every time you just want to throw some files into your cloud storage account. If it's not easy to use, look elsewhere. Reliability: If the cloud storage service shuts down, you may lose all the data. Choose a company that you expect to give your users a fair if they close their doors, or at least offer a way for you to transfer your data elsewhere. Cloud storage services that have been running for a long time or are well known are probably more likely to help if they decide to close the business, but you should read the fine print to see their actual policies. Bandwidth: If you're a heavy user, you should also think about bandwidth limitations. Some cloud storage services cap on how much data can flow in out of your account on a daily or monthly basis. If you plan to have customers, employees, family or friends upload great videos or many other files within a month, make sure the bandwidth cap is not prohibitive for you. You.