WHEN CLOUDS FAIL

Vulnerability of the cloud, not just from a security standpoint but also from an outage perspective, poses bigger challenges for cloud services providers as well as users

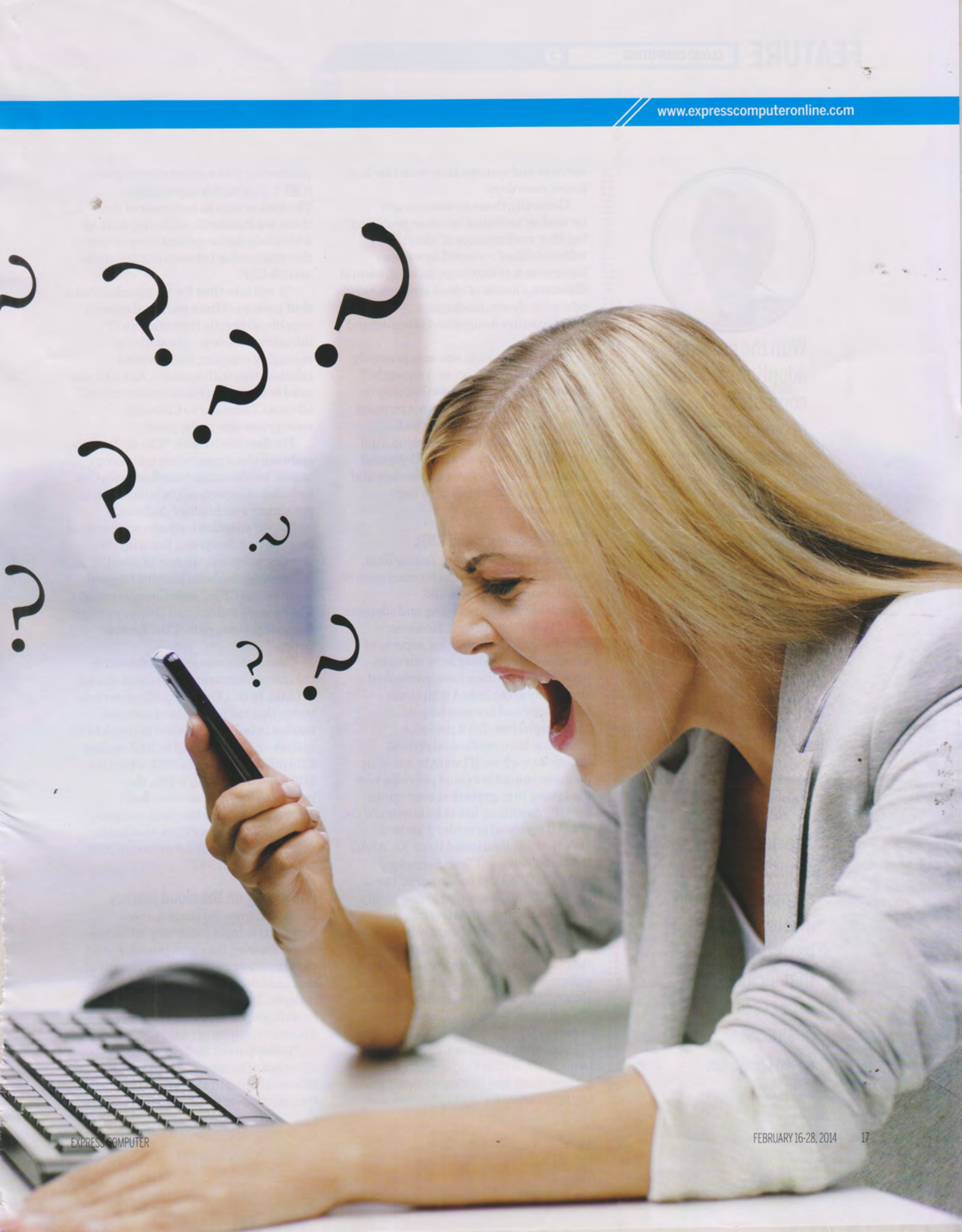
BY PANKAJ MARU

During the early part of December 2013, Yahoo's popular mailing service, Yahoo Mail, remained down for more than 48 hours, causing major problems for a swathe of users and businesses.

It's not the lone incident when a cloud based service suffered huge outage for a long duration.

In fact, the year 2013 saw far too many incidents of cloud disruptions or outages. As per the U.S. based IT continuity management company Neverfail's 2013 Downtime Report, Microsoft's Windows Azure, Google and Amazon Web Services made their way to the top three slots on the list of top 10 outages of the year. The scale of these massive outages was based on the downtime and its overall impact, taking into accounts the lost revenues, expansive reach and damaged reputations due to the downtime.

On many occasions, these tech companies faced technical glitches that caused disruptions of their cloud based



> With the growing adoption of cloud computing, the fear of cloud failures has been looming large on the minds of CIOs.
>
> **Ramesh Babu,**
> Chief Delivery Officer,
> Ramco Systems

> The decision to embrace cloud computing should involve a risk-based analysis that includes all aspects of the business.
>
> **Yateen Chodnekar,**
> Group CIO,
> Writer Corporation

services and systems that lasted for long hours, even days.

Generally, these severances are termed as 'technical issues or problems' but they are instances of 'cloud vulnerabilities' -- caused by various factors such as hardware failures, natural disasters, closure of cloud services, cloud related malware, inadequate infrastructure designs and planning and others.

Arguably, though, one may promptly say, "But they don't occur frequently!" However, the fact remains that they do occur. The possibilities cannot be ruled out in today's time, when almost everything is moving to the cloud. And any kind of downtime caused by 'cloud outage' is detrimental to businesses and enterprises, often leading to huge financial losses.

Cloud economics and CIOs

Although there's the ever lasting data security concerns, given the economics of cloud, most enterprises and organizations are deploying and adopting cloud today than in past. However, 'failures' or 'vulnerabilities' aspects of cloud are going to stay here but to an extent organizations have overlooked those gray areas linked with cloud technology and are vouching on commercial benefits it provides.

"Many have overlooked critical questions such as: If I want to move my business to another cloud provider, how am I going to migrate that over (given that the downtime has to be minimal)? Or, What if my cloud provider goes bust?" says New Zealand based Ryan Ko, APAC Research Adviser, Cloud Security Alliance (CSA) and co-author of the report 'Cloud Computing Vulnerability Incidents: A Statistical Overview.'

While CIOs have always raised the red flag over data and application security in the cloud, the economic pressures to embrace the cloud are too hard to resist. Hence CIOs whether in India or abroad are somehow learning to live with the cloud reality.

According to Yateen Chodnekar, Group CIO, Writer Corporation, vendor management and strategic sourcing are key focus areas for cloud adoption and partnering with a cloud service provider (CSP). Sharing his experiences, Chodnekar says he has ensured that there are standardized, in-depth SLAs which help define critical components of the relationship between organizations and his CSP.

"It will take time for an organization to shift personnel from technical experts capable of directly managing an IT infrastructure to people skilled at managing complex, multifaceted relationships with vendors. As a CIO you need to champion this transformation," advises Chodnekar to CIOs and enterprises new to the cloud.

Further, he stresses, "The decision to embrace cloud computing technology should involve a risk-based analysis that includes all aspects of the business; it is not simply a technology decision."

"Cloud adoption has been accelerating over the past few years. But with the growing adoption, the fear of cloud failures has also been looming large on the minds of CIOs," says Chennai based KM Ramesh Babu, Chief Delivery Officer, Ramco Systems, part of the Ramco Group.

Clearly this scenario is reflected by the momentum seen in the cloud market in India. In fact, Gartner's latest outlook states that the public cloud services market in India is expected to touch $434 million – a 37.5% growth in 2013 against $315 million forecast in 2012, which is a $119 million increase. While, the infrastructure as a service (IaaS) segment that includes cloud compute, storage and print services, that too is expected to touch $62.5 million in 2013 with a jump of 41.8%.

Embarking on the cloud journey

Ironically, from the cloud market perspective India looks very attractive place however, the cloud providers and cloud users or customers are equally at risk and fairly prone to any kind of cloud collapse. This means, they both needs to be well-prepared to face and overcome the consequences of cloud outages.

"It is apparent that cloud failure does affect both the user and the provider. Any failure is bound to affect both the parties. But, most often, failures are because the

business in itself may not be doing too well and not necessarily because of the solution," agrees Babu of Ramco Systems.

Hence, it is important to know and understand how to deal with the scenario of cloud and its vulnerabilities. According to Babu, to overcome cloud failure, one must ensure best practices are adopted right from selecting the cloud application to implementation.

"This includes, doing a complete consulting exercise to identify the right cloud technology for the company, ensuring the solution is a good fit and adopting best practices for a hassle free implementation," informs Babu and further adds that needs a regular review mechanisms to identify any concerns and accordingly take corrective action.

Fortifying the cloud

Since cloud usage has become almost inevitable today, the key to overcome cloud disruptions lies at the very first step when enterprises and organizations decides to accept cloud technology strategically and not just jump on to it, unprepared without any vision.

"But organizations which jump to the cloud, without proper planning and understanding of their business needs are unable to reap the benefits which lead to failures. Some of the most common reasons include poor planning, business unpreparedness, unrealistic expectations and lack of proper training for users, especially in SMB segment," explains Babu, why in some cases, companies face cloud failures.

Further, Babu points that cloud implementations are shorter in duration with little window for recoup, which increases the significance of pre-implementation analysis, complete understanding of the solutions and the risks attached to mitigate them. "It is important that they audit the system and the robustness of the security adapted by the vendor, regularly," he says.

From CIOs perspective, Chodnekar of Writer Corporation points that his focus while adopting cloud in the companies where he worked before has been to ensure a hybrid cloud environments that integrate on-premise and cloud-based applications; and it helps reduce complexity and increase flexibility.

"We integrate in and out of the cloud as necessary to make our processes work, and it has been working quite well for us. I have encouraged my team to invest time in understanding pricing models and increasingly complex cloud service providers solution agreements," Chodnekar says.

"Cloud has long been thought as analogous to electricity, allowing consumers to 'plug-in' and consume IT resources, paying only for what they need. Unfortunately, the IaaS market is far, far away from being a utility, and there is a confusing array of pricing methods, chargeable line items, metrics and pre-configured bundles," Chodnekar highlights other key areas linked with cloud computing.

More so, Chodnekar asks his fellow CIOs and IT decision makers to study the fine print, understand the costs and realistic deliverable, and ensure a tight SLAs and monitoring mechanism to maintain service standards.

"In my view, a proper assessment of the capabilities of the cloud providers (in terms of responding to outages in a transparent and efficient way) would give them a business continuity assurance. After all, the aim of moving to the cloud is to reduce the capital expenditure and increase profits. You do not wish to see some form of 'shocks' after you are well into the business," stresses Ko of CSA.

From cloud user perspective, this is how organizations and enterprises need to plan cloud journey in order to overcome the possibilities of cloud outages or cloud based service disruptions. And this critical situation is no different for the cloud providers that offer cloud services and solutions to large customer base across geographies and regions.

"It all starts with the designing layer of cloud and than its building blocks using best enterprise class infrastructure including hardware components such as storage, compute and networking layers. This helps to build a robust cloud platform and would have minimum failure chances and down time. However, the cloud failure mostly are related to

> A cloud provider must have teams in place for emergency response, crisis management and incident response
>
> **Ryan Ko,**
> APAC Research Adviser,
> Cloud Security Alliance

> While CIOs have always raised the red flag over data and application security in the cloud, the economic pressures to embrace the cloud are too hard to resist

hardware components' failures," says Pune based S S Mulay, Senior Vice President and Head of Engineering and Development, Netmagic Solutions.

In case of Netmagic Solutions, which is a managed and data center services provider, Mulay informs his company uses best of the enterprise class components which includes Cisco's UCS (Unified Computing System) platform, VMware's Hypervisor and storage from NetApp and EMC.

Hardware failure and over-customization

Quite often, the failure is linked with hardware, but for any cloud provider it's a critical state to deal with, considering so many customers of all size and shapes are dependent on the provider's cloud services or enterprise applications are running on that cloud.

Given this scenario, the cloud providers needs to have enough resources, equipped with technology to react promptly, in case of cloud outages and reduce the impact on businesses in possible shortest time. Besides, they need to have back-up support systems that enables businesses continuity for their customers with certain level of surety, under defined service level agreements (SLAs) and contracts.

"Though these enterprise class or best of breed type hardware have very low failure rates but any kind of hardware remains prone to failures. Even when there's hardware (blade or chassis) failure, if there are clusters in place spanning across multiple chassis, or even if an entire chassis goes down, it doesn't really cause much of an impact to our customers," explains Mulay.

"Secondly, all the clusters we have, are designed in such a way that there are extra resources available in standby. This can easily fill in the gap, if one or two VMs (virtual machines) bursts as there's enough capacity available across the gird, without reducing the performance and the customers doesn't even feel its impact," adds Mulay, how the technical arrangements can lower the cloud failures and its impact.

Besides the hardware failure, being one of the reason for cloud outages, it's the over-customization of cloud that is responsible for cloud disruptions and its massive impact. While, hardware breakdowns are highly predictable, in Mulay's opinion about 20% cloud outages are triggered by hardware but its the layer customization that causes bigger damage or impact of cloud collapse than the hardware.

Since the occurrence of incidents have gone up over the years, it is important to know the reasons behind cloud outages and how cloud providers are responding

Compared to hardware, the layer customization or automation triggers cloud outages and its impact is far greater as customization weaken overall controls and down-time can last for longer duration.

But the fact remains that today most cloud providers bank on customized services to drive business and trying to meet their customer needs. Many cloud provider are guilty of over customization or automation of some layers like hypervisor or virtualization layer, which in simple terms, is pushing beyond the limits and capabilities what the platform or framework offers.

Such extreme tweaks can easily create enormous pressure on the layers or platforms and henceforth it manipulate the functional capabilities. Though it results into partial kind of

failures of cloud services, but the impacts are very high.

"Providing customization to customers within the framework limits to an extent is acceptable, however when there's over customization and also some time even service providers make internal changes to platforms, which more likely causes the cloud disruptions," points out Mulay.

Going back to SLAs, Netmagic claims to offers 99.99% SLAs on the availability of the VMs due to its latest cloud technology compared to competitors that over availability on the networks to customers. Company's over all business is growing more than 200% compared to cloud business, which has moved to 8% from 1% some three years ago.

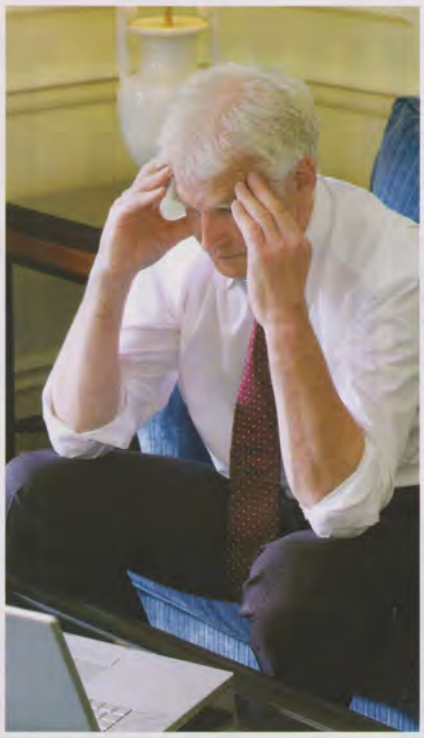
Public clouds highly prone

According to Cloud Security Alliance (CSA)'s Cloud Vulnerabilities Working Group report titled - 'Cloud Computing Vulnerability Incidents: A Statistical Overview'– during a span of five years between January 2008 and February 2012, the number of cloud vulnerability incidents rose considerably. The report is based on the number of reported incidents in the media.

The count of cloud vulnerability incidents has more than doubled over a four year period, from 33 in 2009 to 71 in 2011 and a total of 172 unique cloud computing outage incidents were uncovered, of which 129 (75%) declared their causes while 43 (25%) did not, the report states.

Since the occurrence of incidents have gone up over the years, it is important to know and understand what are reasons triggering to cloud outages and also how cloud providers and organizations are responding to the situation.

Ko, who co-authored the CSA report along with Singapore based Stephen Lee and V Rajan from Nanyang Technological University, says that the top causes found in the report were 'Insecure Interfaces & APIs' (29%), closely followed by 'Data Loss & Leakage' (25%). He points out, "These two categories shows there is a need to develop cloud software with security in mind, from the ground up."



Both cloud providers as well as its users (enterprises) are prone to disruptions or outages, there is a need of mutual understanding and technical response mechanism to address the situation of cloud severances.

"The first thing that they need to do is to look at developing mutually beneficial SLA and contracts. Only after that, the service agreements will come in play. All organizations must check to see if their cloud providers have (at a minimum) the following teams in place: Emergency Response Team (ERT), Crisis Management Team and an Incident Response Team. Without these teams, it is hard to see how a cloud provider can deal with a crisis and ensure fast recovery in the event of a major failure," explains Ko, who is also a Computer Science professor at University of Waikato, New Zealand.

"There is no room for relaxing and complacency which often results in failures. Information Technology is a serious business and only those who have the ability and wiliness with a long term vision should enter it," comments Chodnekar of Writer Corporation

Interestingly, the CSA report has more references and details of cloud outage incidents largely from the U.S and Europe, compared to Asia including India, where the cloud market is growing fast than other regions in the world.

"I believe that has got to do with the legal requirements. In most western countries, especially those in the European Union, strict regulations are placed so that the cloud providers are regulated in a compliant manner," reasons Ko, why his report has more clouds outage incidents from the west compared to Asia.

Further, Ko points that Asian countries lack government legislation linked with the cloud computing industry. "When such mandates are in place, Asian cloud providers will have to conform and report outages in a more transparent manner - which ultimately benefits the cloud customers. Aside from legislation, efforts such as CSA STAR (Security, Trust & Assurance Registry) and OCF (Open Certification Framework) are great ways to assure high quality and highly-accountable clouds."

In Asia, India has a highly growing cloud ecosystem including the vendors, cloud services providers as well as the users (enterprises and organizations); however, there have been no reported incidents of cloud outages so far.

"There has been better awareness on the expectations from cloud. This is because most often we see that cloud adoption is always business-driven rather than being IT-driven. The maturity of providers and enterprises is high, leading to better managed projects. Also, the organization as well as the service providers have put in place best practices to ensure the desired outcome," says Babu.

The probability of failures is much more for public clouds compared to private ones, but if best practices are followed—right from robust designing, hardware resource allocations as well as utilization of resources and platforms, controls on layers and infrastructure—it can minimize the possibilities of cloud outages to a great extent.

pankaj.maru@expressindia.com