International Journal of Technical Research and Applications e-ISSN: 2320-8163,
www.ijtra.com Volume 2, Issue 6 (Nov-Dec 2014), PP. 143-148

SECURITY ISSUES IN CLOUD COMPUTING

Nitin Kumar Upadhyay[1]
O.P Jindal Institute of Technology, Raigarh
nitin.upadhyay@opjit.edu.in

Dr Ashok Bhansali[2]
O.P Jindal Institute of Technology, Raigarh
ashok.bhansali@opjit.edu.in

Manish Kumar Upadhyay[3]
SPNJ India Ltd., Raipur
manish14061984@gmail.com

Abstract- Cloud computing is architecture for providing computing service via the internet on demand and pay per use access to a pool of shared resources namely networks, storage, servers, services and applications, without physically acquiring them. So it saves managing cost and time for organizations. The market size the cloud computing shared is still far behind the one expected. From the consumers' perspective, cloud computing security concerns, especially data security and privacy protection issues, remain the primary inhibitor for adoption of cloud computing services. The security for Cloud Computing is emerging area for study and this paper provide security topic in terms of cloud computing based on analysis of Cloud Security treats and Technical Components of Cloud Computing.

I. Introduction

Cloud computing represents significant opportunity for service providers and enterprises relying on the cloud computing, enterprises can achieve cost savings, flexibility, and choice for computing resources. They are looking to expand their on-promise infrastructure, by adding capacity on demand. Cloud computing, most, simply, extends an enterprise's ability to meet the computing demands of its everyday operation. Offering flexibility and choice, mobility and scalability, all coupled with potential cost savings, there is significant benefit to leveraging cloud computing. However, the area is causing organizations to hesitate most when it comes to moving business workloads into public cloud is security.

A. Technical Components of Cloud Computing

A key function of a cloud management system is divided into four layers, respectively the Resources & Network Layer, Services Layer, Access Layer, and User Layer. Each layer includes a set of functions:

1. The Resources & Network Layer manages the physical and virtual resources.
2. The Services Layer includes the main categories of cloud services, namely, NaaS, IaaS, PaaS, SaaS/CaaS, the service orchestration function and the cloud operational function.
3. The Access Layer includes API termination function, and Inter-Cloud peering and federation function.
4. The User Layer includes End-user function, Partner function and Administration function.

Other functions like Management, Security & Privacy, etc. are considered as cross-layer functions that covers all the layers. The main principle of this architecture is that all these layers are supposed to be optional. This means that a cloud provider who wants to use the reference architecture may select and implement only a subset of these layers.

However, from the security perspective, the principal of separation requires each layer to take charge of certain responsibilities. In event the security controls of one layer are by passed (e.g. access layer), other security functions could compensate and thus should be implemented either in other layers or as cross-layer functions.

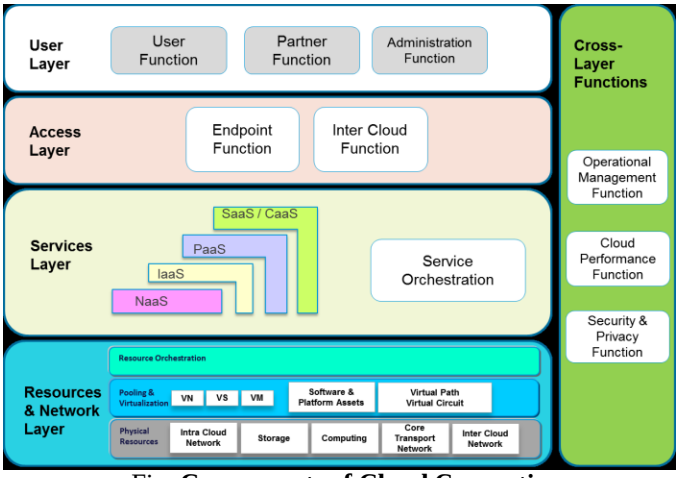

Fig: **Components of Cloud Computing**

B. The cloud computing opportunity

Several points that attract enterprises and organization to move to the cloud computing that's why the following opportunities in the cloud computing is considered.

Industrial momentum: industry analysts and companies like Amazon, Citrix, Dell, Google, HP, IBM, Microsoft, Sun, VMware and many others appears greatly in support of cloud computing. In September 2008, the VMware v Cloud was the first example of a technology vendor bringing service providers, applications and technologies together to increase the availability and opportunity for enterprises to leverage cloud computing.

Flexibility: Enterprises can choose to outsource hardware while maintaining control of their IT infrastructure; they can fully-outsource all aspects of their infrastructure; or, often driven by departmental initiatives, enterprises are deploying both fully and partially-outsourced segments of their infrastructures.

Cost Savings: Infrastructure on demand leads to more efficient IT spending. Restriction on headcount and capital expenditures often back innovation seasonal demands spike capacity requirements and require a robust infrastructure that is frequently unutilized. Cloud computing is a cost-effective alternative.

Mobility and Choice: Technology is leading the evolution.

Virtualization technologies like VMware enables applications and services to be moved from internal environments to public clouds or from one cloud service provider to another.

Scalability: Infrastructure as a Service (Iaas) synonymous with scalability. Failover and redundancy are also high-impact opportunities to leverage cloud computing.

II. Essential characteristics

On-demand capabilities: A business will secure cloud-hosting services through a cloud host provider which could be your usual software vendor. You have access to your services and you have the power to change cloud services through an online control panel or directly with the provider. You can add or delete users and change storage networks and software as needed. Typically, you are billed with a monthly subscription or a pay-for-what-you-use scenario. Terms of subscriptions and payments will vary with each software provider.

Broad network access:
Your team can access business management solutions using their smartphones, tablets, laptops, and office computers. They can use these devices wherever they are located with a simple online access point. This mobility is particularly attractive for businesses so that during business hours or on off-times, employees can stay on top of projects, contracts, and customers whether they are on the road or in the office. Broad network access includes private clouds that operate within a company's firewall, public clouds, or a hybrid deployment.

Resource pooling:
The cloud enables your employees to enter and use data within the business management software hosted in the cloud at the same time, from any location, and at any time. This is an attractive feature for multiple business offices and field service or sales teams that are usually outside the office

Rapid elasticity:
If anything, the cloud is flexible and scalable to suit your immediate business needs. You can quickly and easily add or remove users, software features, and other resources.

Measured service:
Going back to the affordable nature of the cloud, you only pay for what you use. You and your cloud provider can measure storage levels, processing, bandwidth, and the number of user accounts and you are billed appropriately.

Security Concerns

However the cloud computing is attracting the enterprises and organizations to
move, but the some concerns for the enterprises and organization has to keep in mind for their virtual infrastructure. These concerns which identify the security issues in cloud computing are as follows:

Where's the data? :
Deferent countries have deferent requirements and controls placed on access.

Who has access? :
Access control is a key concern, because insider attacks are a huge risk. A potential hacker is someone who has been interested with approved access to the cloud.

What are your regulatory requirements? :
Organizations operating in the US, Canada , or the European Union have many regulatory requirements that they must abide by (e.g., ISO 27002, Safe Harbor, ITIL, and COBIT).

Do you have the right to audit? :
This particular item is no small matter; the cloud provider should agree in writing to the terms of audit.

What type of training does the provider over their employees? :
This is actually a rather important item, because people will always be the weakest link in security. Knowing how your provider trains their employees is an important item to review.

What type of data classification system does the provider use? :
Is the data classified? How is your data separated from other users? Encryption should also be discussed. Is it being used while the data is at rest or in transit?

What are the service level agreement (SLA) terms?:
The SLA serves as a contracted level of guaranteed service between the cloud provider and the customer that specifies what level of services will be provided.

III. Threats for Cloud Service Users

A. Responsibility Ambiguity

Cloud service users consume delivered resources through service models. The customer-built IT system thus relies on the services. The lack of a clear definition of responsibility among cloud service users and Providers may evoke conceptual conflicts. Moreover, any contractual inconsistency of provided services could induce anomaly, or incidents. However the problem of which entity is the data controller which on is the data processor stays open at an international scale (even if the international aspect is reduced to a minimal third party outside of the specific region like EU).

B. Loss of Governance

For an enterprise, migrating a part of its own IT system to a cloud infrastructure implies to partially give control to the cloud service providers. This loss of governance depends on the cloud service models. For instance, IaaS only delegates hardware and network management to the provider, while SaaS also delegates OS, application, and service integration in order to provide a turnkey service to the cloud service user.

C. Loss of Trust

It is sometime difficult for a cloud service user to recognize his provider's trust level due to the black-box feature of the cloud service. There is no measure how to get and share the provider's security level in formalized manner. Furthermore, the cloud service users have no abilities to

evaluate security implementation level achieved by the provider. Such a lack of sharing security level in view of cloud service provider will become a serious security threat in use of cloud services for cloud service users.

D. Service Provider Lock-in

A consequence of the loss of governance could be a lack of freedom regarding how to replace a cloud provider by another. This could be the case if a cloud provider relies on non-standard hypervisors or virtual machine image format and does not provide tools to convert virtual machines to a standardized format.

E. Unsecure Cloud Service User Access

As most of the resource deliveries are through remote connection, non-protected APIs, (mostly management APIs and PaaS services is one of the easiest attack vector). Attack methods such as phishing, fraud, and exploitation of software vulnerabilities still achieve results. Credentials and passwords are often reused, which amplifies the impact of such attacks. Cloud solutions add a new threat to the landscape. If an attacker gains access to your credentials, they can eavesdrop on your activities and transactions, manipulate data, return falsified information, and redirect your clients to illegitimate sites. Your account or service instances may become a new base for the attacker. From here, they may leverage the power of your reputation to launch subsequent attacks.

F. Lack of Information/Asset Management

When applying to use Cloud Computing Services, the cloud service user will have serious concerns on lack of information/asset management by cloud service providers such as location of sensitive asset/information, lack of physical control for data storage, reliability of data backup (data retention issues), countermeasures for BCP and Disaster Recovery and so on. Furthermore, the cloud service users also have important concerns on exposure of data to foreign government and on compliance with privacy law such as EU data protection directive.

G. Data loss and leakage

The loss of encryption key or privileged access code will bring serious problems to the cloud service users. Accordingly, lack of cryptographic management information such as encryption keys, authentication codes and access privilege will heavily lead sensitive damages on data loss and unexpected leakage to outside. For example, insufficient authentication, authorization, and audit (AAA) controls; inconsistent use of encryption and/or authentication keys; operational failures; disposal problems; jurisdiction and political issues; data center reliability; and disaster recovery can be recognized as major behaviors in this threat category.

IV. Threats for Cloud Service Providers

A. Responsibility Ambiguity

Different user roles, such as cloud service provider, cloud service user, client IT admin, data owner, may be defined and used in a cloud system. Ambiguity of such user roles and responsibilities definition related to data ownership, access control, infrastructure maintenance, etc, may induce business or legal dissention (Especially when dealing with third parties. The cloud service provider is somehow a cloud service user).

B. Protection Inconsistency

Due to the decentralized architecture of a cloud infrastructure, its protection mechanisms are likely to be inconsistency among distributed security modules. For example, an access denied by one IAM module may be granted by another. This threat may be profited by a potential attacker which compromises both the confidentiality and integrity.

C. Evolutional Risks

One conceptual improvement of cloud computing is to postpone some choices from the design phase to the execution phase. This means, some dependent software components of a system may be selected and implemented when the system executes. However, conventional risk assessment methodology can no longer match such an evolution. A system which is assessed as secure during the design phase may exploit vulnerabilities during its execution due to the newly implemented software components.

D. Business Discontinuity

The "as a service" feature of cloud computing allocates resources and delivers them as a service. The whole cloud infrastructure together with its business workflows thus relies on a large set of services, ranging from hardware to application. However, the discontinuity of service delivery, such as black out or delay, may bring out a severe impact related to the availability.

E. Supplier Lock-in

The platform of a service provider is built by some software and hardware components by suppliers. Some supplier-dependent modules or workflows are implemented for integration or functionality extension. However, due to the lack of standard APIs, the portability to migrate to another supplier is not obvious. The consequence of provider locked-in could be a lack of freedom regarding how to replace a supplier.

F. License Risks

Software licenses are usually based on the number of installations, or the numbers of users. Since created virtual machines will be used only a few times, the provider may have to acquire from more licenses than really needed at a given time. The lack of a "clouded" license management scheme which allows to pay only for used licenses may cause software use conflicts.

G. Bylaw Conflict

Depending on the bylaw of hosting country, data may be protected by different applicable jurisdiction. For instance, the USA Patriot Act may authorize such seizures. EU protects cloud service user's private data, which should not be processed in countries that do not provide a sufficient level of protection guarantees. An international cloud service provider may commit bylaws of its local datacenters which is a legal threat to be taken into account.

H. Bad Integration

Migrating to the cloud implies moving large amounts of data and major configuration changes (e.g., network addressing). Migration of a part of an IT infrastructure to an external cloud service provider requires profound changes in the infrastructure design (e.g. network and security policies). A bad integration caused by incompatible interfaces or inconsistent policy enforcement may evoke both functional and non-functional impacts.

I. Unsecure Administration API

The administration middleware standing between the cloud infrastructure and the cloud service user may be not sure with insufficient attention devoted to sanitation of cloud service user inputs and authentication. Non-protected APIs, mostly administration APIs becomes a target of choice for attackers. This is not specific to cloud environment. However, the service-oriented approach makes APIs a basic building block for a cloud infrastructure. Their protection becomes a main concern of the cloud security.

J. Shared Environment

Cloud resources are virtualized, different cloud service users (possibly competitors) share the same infrastructure. One key concern is related to architecture compartmentalization, resource isolation, and data segregation. Any unauthorized and violent access to cloud service user's sensitive data may compromise both the integrity and confidentiality.

K. Hypervisor Isolation Failure

The hypervisor technology is considered as the basis of cloud infrastructure. Multiple virtual machines co-hosted on one physical server share both CPU and memory resources which are virtualized by the hypervisor. This threat covers the failure of mechanisms isolating attack" could be launched on a hypervisor to gain illegal access to other virtual machines' memory.

L. Service Unavailability

Availability is not specific to cloud environment. However, because of the service-oriented design principle, service delivery may be impacted while the cloud infrastructure in not available. Moreover, the dynamic dependency of cloud computing offers much more possibilities for an attacker. A typical Denial of Service attack on one service may clog the whole cloud system.

M. Data Unreliability

Data protection includes access to data for the confidentiality as well as its integrity. Cloud service users have concerns about how providers handle with their data, and whether their data is disclosed or illegally altered. Even if the cloud service user trust is not in the central of cloud security, it is a major marketing differentiator for a cloud service provider to advance the migration of IT system to cloud environment.

N. Abuse Right of Cloud Service Provider

For a cloud service user, migrating a part of its own IT to a cloud infrastructure implies to partially give control to the provider. This becomes a serious threat to cloud service user's data, notably regarding role and privileges assignment to providers. Coupled with lack of transparency regarding cloud provider practices may conduce mis-configuration or malicious insider attack. Such security breaches will lower the provider's reputation, resulting in lower cloud service user confidence.

O. Security Issues in SaaS

Following key security element should be carefully considered as an Integral part of the SaaS deployment process:

1. Data Security
2. Network Security
3. Data locality
4. Data integrity
5. Data access
6. Data Segregation
7. Authorization and Authentication
8. Data Confidentiality
9. Web Application security
10. Data Breaches
11. Virtualization vulnerability
12. Availability
13. Backup
14. Identity Management on sign-on process

Security Issues in PaaS

1. In PaaS, the provider might give some control to the people to build applications on top of the platform. But any security below the application level such as host and network intrusion prevention will still be in the scope of the provider.

2. Applications sufficiently complex to leverage an Enterprise Service Bus (ESB) need to secure the ESB directly, leveraging a protocol such as Web Service (WS) Security (Oracle, 2009).The ability to segment ESBs is not available in PaaS environments. Metrics should be in place to assess the effectiveness of the application security programs.

3. Hackers are likely to attack visible code, including but not limited to code running in user context. They are likely to attack the infrastructure and perform extensive black box testing. The vulnerabilities of cloud are not only associated with the web applications but also vulnerabilities associated with the machine-to-machine Service Oriented Architecture (SOA) applications.

Security Issues in IaaS

Taking virtual machines, which contain critical applications and sensitive data, off premise to public and shared cloud environments creates security challenges for organizations that have relied on network perimeter defense as the main method to protect their datacenter. It may also revoke compliance and breach security policies.

OS Security issues also alive in IaaS. Following are the points which are considered in IaaS.

V. Cloud security challenges

The current adoption of cloud computing is associated with numerous challenges because users are still skeptical about its authenticity. Based on a survey conducted by IDC in 2008, the major challenges that prevent Cloud Computing from being adopted are recognized by organizations are as follows:

A. Security:

It is clear that the security issue has played the most important role in hindering Cloud computing acceptance. Without doubt, putting your data, running your software on someone else's hard disk using someone else's CPU appears daunting to many. Well-known security issues such as data loss, phishing, botnet (running remotely on a collection of machines) pose serious threats to organization's data and software. Moreover, the multi-tenancy model and the pooled computing resources in cloud computing has introduced new security challenges that require novel techniques to tackle with. For example, hackers can use Cloud to organize botnet as Cloud often provides more reliable infrastructure services at a relatively cheaper price for them to start an attack.

B. Costing Model:

Cloud consumers must consider the tradeoffs amongst computation, communication, and integration. While migrating to the Cloud can significantly reduce the infrastructure cost, it does raise the cost of data communication, i.e. the cost of transferring an organization's data to and from the public and community Cloud and the cost per unit of computing resource used is likely to be higher. This problem is particularly prominent if the consumer uses the hybrid cloud deployment model where the organization's data is distributed amongst a number of public/private (in-house IT infrastructure)/community clouds. Intuitively, ondemand computing makes sense only for CPU intensive jobs.

C. Charging Model:

The elastic resource pool has made the cost analysis a lot more complicated than regular data centers, which often calculates their cost based on consumptions of static computing. Moreover, an instantiated virtual machine has become the unit of cost analysis rather than the underlying physical server. For SaaS cloud providers, the cost of developing multitenancy within their offering can be very substantial. These include: re-design and redevelopment of the software that was originally used for single-tenancy, cost of providing new features that allow for intensive customization, performance and security enhancement for concurrent user access, and dealing with complexities induced by the above changes. Consequently, SaaS providers need to weigh up the trade-off between the provision of multitenancy and the cost-savings yielded by multi-tenancy such as reduced overhead through amortization, reduced number of on-site software licenses, etc. Therefore, a strategic and viable charging model for SaaS provider is crucial for the profitability and sustainability of SaaS cloud providers.

D. Service Level Agreement (SLA):

Although cloud consumers do not have control over the underlying computing resources, they do need to ensure the quality, availability, reliability, and performance of these resources when consumers have migrated their core business functions onto their entrusted cloud. In other words, it is vital for consumers to obtain guarantees from providers on service delivery. Typically, these are provided through Service Level Agreements (SLAs) negotiated between the providers and consumers. The very first issue is the definition of SLA specifications in such a way that has an appropriate level of granularity, namely the tradeoffs between expressiveness and complicatedness, so that they can cover most of the consumer expectations and is relatively simple to be weighted, verified, evaluated, and enforced by the resource allocation mechanism on the cloud. In addition, different cloud offerings (IaaS, PaaS, and SaaS) will need to define different SLA meta specifications. This also raises a number of implementation problems for the cloud providers. Furthermore, advanced SLA mechanisms need to constantly incorporate user feedback and customization features into the SLA evaluation framework.

E. What to migrate:

Based on a survey (Sample size = 244) conducted by IDC in 2008, the seven IT systems/applications being migrated to the cloud are: IT Management Applications(26.2%), Collaborative Applications (25.4%), Personal Applications (25%), Business Applications (23.4%), Applications Development and Deployment (16.8%), Server Capacity (15.6%), and Storage Capacity (15.5%). This result reveals that organizations still have security/privacy concerns in moving their data on to the Cloud. Currently, peripheral functions such as IT management and personal applications are the easiest IT systems to move. Organizations are conservative in employing IaaS compared to SaaS. This is partly because marginal functions are often outsourced to the Cloud, and core activities are kept in-house. The survey also shows that in three years time, 31.5% of the organization will move their Storage Capacity to the cloud. However this number is still relatively low compared to Collaborative Applications (46.3%) at that time.

F. Cloud Interoperability Issue:

Currently, each cloud offering has its own way on how cloud clients/applications/users interact with the cloud, leading to the "Hazy Cloud" phenomenon. This severely hinders the development of cloud ecosystems by forcing vendor locking, which prohibits the ability of users to choose from alternative vendors/offering simultaneously in order to optimize resources at different levels within an organization. More importantly, proprietary cloud APIs makes it very difficult to integrate cloud services with an organization's own existing legacy systems (e.g. an on-

premise data centre for highly interactive modeling applications in a pharmaceutical company).The primary goal of interoperability is to realize the seamless fluid data across clouds and between cloud and local applications. There are a number of levels that interoperability is essential for cloud computing. First, to optimize the IT asset and computing resources, an organization often needs to keep in-house IT assets and capabilities associated with their core competencies while outsourcing marginal functions and activities (e.g. the human resource system) on to the cloud. Second, more often than not, for the purpose of optimization, an organization may need to outsource a number of marginal functions to cloud services offered by different vendors. Standardization appears to be a good solution to address the interoperability issue. However, as cloud computing just starts to take off, the interoperability problem has not appeared on the pressing agenda of major industry cloud vendors. S. Ramgovind, M. M. Eloff, E. Smith. "The Management of Security in Cloud Computing" In PROC 2010 IEEE International Conference on Cloud Computing 2010

G. Solution approaches:

The following outlines four distinct security technologies –firewall, intrusion detection and prevention, integrity monitoring and log inspection- that can be deployed as software on virtual machines to increase protection and maintain compliance integrity of servers and applications as virtual resources move from on-premise to public cloud environment

VI. Firewall

Decreasing the attack surface of virtualized servers in cloud computing environments. A bi-directional firewall, deployed on individual virtual machines can provide centralized management of server firewall policy. It should include predefined templates for common enterprise server types and enable the following:

1. Virtual machine isolation
2. Fine-grained filtering(Source and Destination Address, Ports)
3. Coverage of all IP-based protocols (TCP, UDP, ICMP, …)
4. Coverage of all frame types (IP, ARP, …)
5. Prevention of Denial of Service (DoS) attacks
6. Ability to design policies per network interface
7. Location awareness to enable tightened policy and the flexibility to move the virtual machine from on-premise to cloud resources

VII. Intrusion Detection and Prevention (IDS/IPS)

Shield vulnerabilities in operating system and enterprise applications until they can be patched, to achieve timely protection against known and zero-day attacks. As previously noted, virtual machines and cloud computing servers use the same operating systems, enterprise and web applications as physical servers. Deploying intrusion detection and prevention as software on virtual machines shields newly discovered vulnerabilities these applications and OSs to provide protection against exploits attempting to compromise virtual machines.

A. Integrity Monitoring

Integrity monitoring of critical operating system and application files (files, directories, registry keys and values, etc.) is necessary for detecting malicious and unexpected changes which could signal compromise of cloud computing resources. Integrity monitoring software must be applied at the virtual machine level.

B. Log Inspection

Log inspection collects and analyzes operating system and application logs for security events. Log inspection rules optimize the identification of important security events buried in multiple log entries. These events can be sent to a stand-alone security system, but contribute to maximum visibility when forwarded to a security Information and event management (SIEM) system or centralized logging server for correlation, reporting and archiving. Like integrity monitoring, log inspection capabilities must be applied at the virtual machine level. Log inspection software on cloud resources enables:

1. Suspicious behavior detection
2. Collection of security-related administrative actions
3. Optimized collection of security events across your datacenter

VIII. Conclusion

After discussing the security issues this paper conclude that we should be careful about the security concerns while putting our business on Cloud. Cloud computing is no exception. In this paper key security considerations and challenges which are currently faced in the Cloud computing are highlighted. Cloud computing has the potential to become a frontrunner in promoting a secure, virtual and economically viable IT solution in the future. In any cloud service (infrastructure, software or platform) the end service provider or enterprise will control the access to the services.

REFERENCES

[1] Rabi Prasad Padhy,Manas Ranjan Patra,Suresh Chandra Satapathy "Cloud Computing:Security Issue and research challanges", IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS) Vol. 1, No. 2, December 2011.

[2] Kangchan Lee" Security Threats in Cloud Computing Environments1" , International Journal of Security and Its Applications Vol. 6, No. 4, October, 2012.

[3] www.cloudsecurityalliance.org/guidance

[4] Deyan Chen, Hong Zhao "Data security & Privacy Protection issues in cloud computing",2012 international conference on computer science & electronic engineering.

[5] http://erpbloggers.com/2013/07/the-five-essential-characteristics-of-cloud-computing/#sthash.hFuPaJIE.dpuf