TECHNOLOGY SCAN:
CLOUD SECURITY

IPOS
INTELLECTUAL PROPERTY
OFFICE OF SINGAPORE

IPOS
international

WITH INPUT FROM

GOVTECH
SINGAPORE

DISCLAIMER

The information, analysis, and opinions (the "Content") contained herein are based on information reasonably available and accessible as of the date of the analysis. While IPOS endeavours to ensure that the Content is correct as of the date of the analysis, IPOS does not warrant the accuracy or completeness of the Content. The Content in this report does not constitute any legal, business or financial advice and nothing contained herein shall be construed as such. Neither IPOS nor any of its affiliates shall be liable for any claims, expenses or liabilities which may arise from this report.

COPYRIGHT NOTICE

METHODOLOGY

1. Dataset used for the report

The patent dataset was retrieved on 26 February 2019 and comprises worldwide patent applications relating to cloud security technologies published in 2009-2018.

Relevant business information, market data, and national policies that are available from commercial databases or on the web are also used to support the findings of the report.

2. Counting the number of inventions

This report counts the number of inventions by the number of unique patent families. Counting individual patent applications will result in double counting as each patent family may contain several patent publications if the applicant files the same invention for patent protection in multiple destinations. As a patent family is a group of patent applications relating to the same invention, analyses based on counting one invention per unique patent family can reflect innovation activity more accurately.

3. Formulation of search strings

To ensure optimal recall and accuracy of the data sets retrieved, the search strings used in this study were formulated by incorporating keywords (and their variants), as well as relevant patent classification codes and indexes, e.g. International Patent Classification (IPC) and Cooperative Patent Classification (CPC).

4. Grouping of technology domains

Grouping of individual patent documents into the respective technology domains was carried out based on patent classifications codes, text-mining and semantic analysis of the patent specifications in particular claims, titles, abstracts, as well as a manual review of the individual patent applications.

5. Growth rate calculation

Annual growth rate refers to the average annual growth and was derived by using the best-fit exponential line method for the set of data, $y = a*e^{bx}$, where b is the growth rate.

CONTENTS

INTRODUCTION

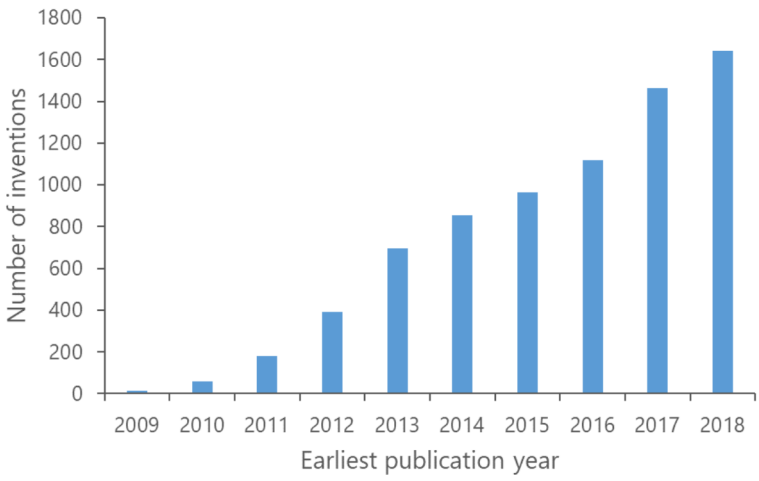
Marriott Starwood hotels. Quora. Facebook. Google+. Timehop. Microsoft Office 365. Box.

These were some of the biggest names that have fallen victims to cloud-related security breaches in recent years.[1,2] As more organisations join the ever-growing list of victims,[1,2] many of such cyber threats are on-going and may remain undetected. For industries which are keen adopters of cloud technology, incidents of security breaches can be costly.[3,4] Monetary loss aside, concerns over the organisation's reputation and consumer confidence are some of the aftermath issues that organisations will urgently need to address.

Nevertheless, the adoption of cloud-based solutions by organisations will only increase in the current digitisation-powered Industry 4.0 era. Driven by financial and espionage motives, the cloud, with its increasing mass of confidential data, thus represents an attractive target for hackers, who constantly modify their modes of attack to steal invaluable information.[5]

Hence, threats to cloud platforms demand attention from both service providers and consumers of cloud technology. Solutions to tackle these threats are a major consideration for further applications of cloud technologies. Consequently, innovators are actively confronting these challenges head-on by pursuing new innovations to thwart the work of hackers and attackers. Given the pertinent need to understand innovative methods to ensure cloud safety, this report looks at worldwide patent applications relating to cloud security published in 2009-2018 with a particular focus in the areas of (a) identity and access management; (b) data security; (c) network security; (d) virtualisation security; and (e) security policy management, to understand the current technologies in cloud security.

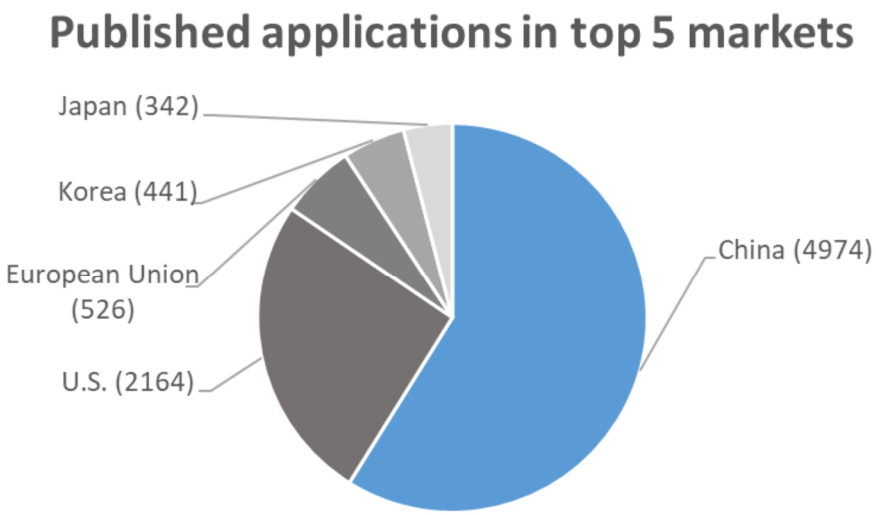
INCREASING INNOVATION INTEREST IN CLOUD SECURITY



The number of published patent applications worldwide relating to innovations on cloud security totalled 7396 during the surveyed period of 2009-2018. A huge interest in cloud security was further substantiated by innovation interest over the recent five years, with an annual growth rate of 17.3%. Supported by the growing demand of cloud services, the global cloud security market is expected to hit approximately USD 13 billion by 2022, with a compounded annual growth rate (CAGR) of 17%.[6] With burgeoning cloud adoptions set to grow into the next decade, innovation activities into defending the integrity of cloud platforms are also expected to follow.

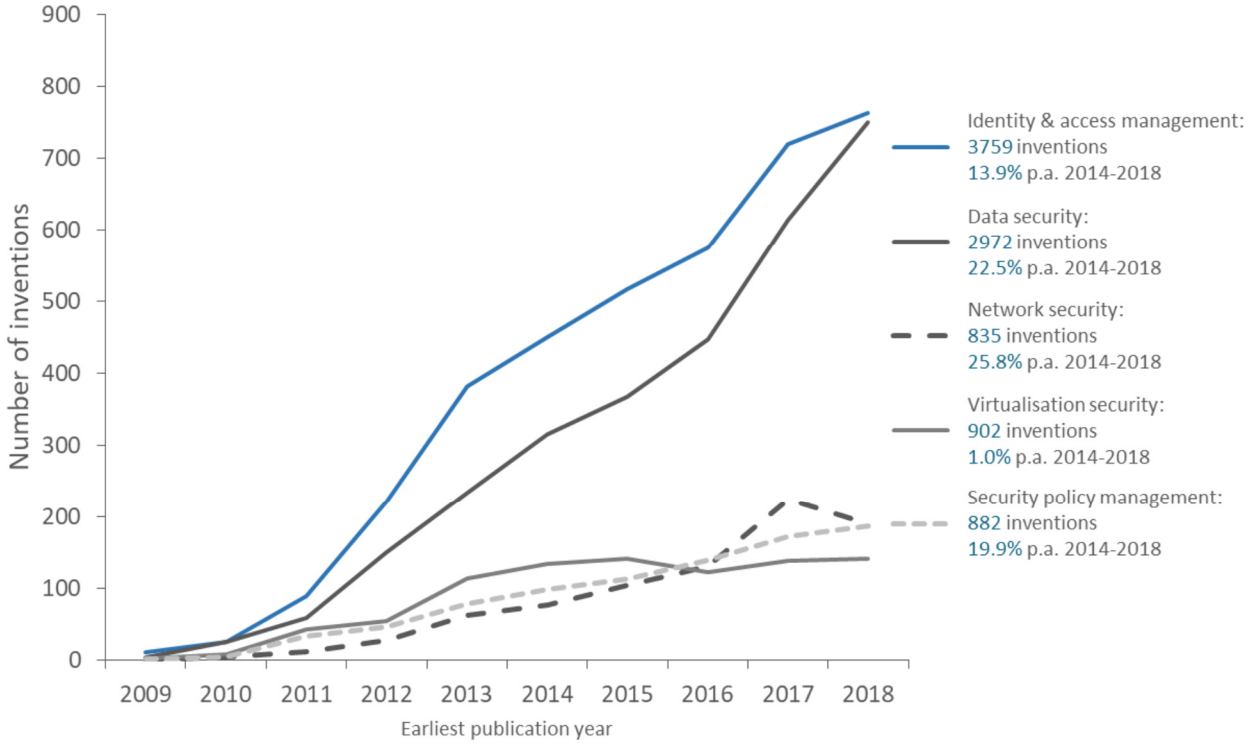
CHINA IS THE LEADING MARKET FOR PATENT PROTECTION

While cloud deployment has been known to be prevalent in the U.S. market, the Asian giant, China, is awakening and looking towards opening up and accelerating towards cloud usage.[7] As such, it is hardly surprising to see a large growth in interest in seeking protection of cloud security inventions in China. Specifically, the number of patents seeking protection in China alone has surpassed the rest of the world combined.



This has been partially attributed to the efforts of the Chinese government, which has recognised the value of cloud computing and committed to expanding China's cloud computing scale by 2.5 times from 2015 to 2019.[8] This has resulted in recent growing interest in protection of cloud security inventions in China, with a publication rate of 23.3% per annum in the recent 5 years. With the regulatory push towards adoption of cloud computing, coupled with the on-going large-scale cloud development spearheaded by Alibaba in China,[9,10] it is foreseeable that China will be an important market for cloud security solutions for many years to come.

IDENTITY & ACCESS MANAGEMENT AND DATA SECURITY TAKE THE LEAD



Cloud security can be partitioned into five main aspects:

i) *Identity and access management*[i];

ii) *Data security*[ii];

iii) *Network security*[iii];

iv) *Virtualisation security*[iv];

v) *Security policy management*[v].

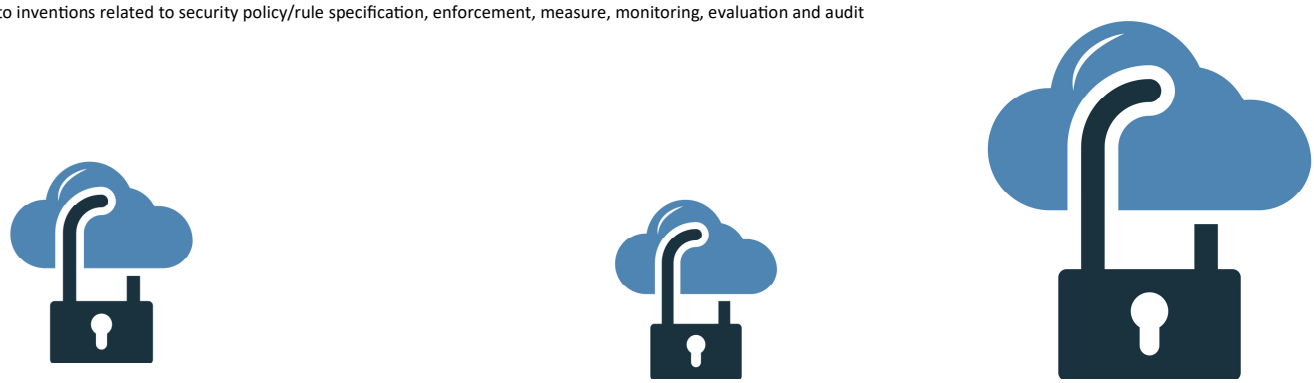
[i] generally refers to inventions for tracking, controlling and managing user identities and access privileges for various resources, including access control, identity provisioning, identity authentication and authorisation

[ii] comprises a variety of inventions for protecting the security of data on cloud, such as data encryption, hashing, digital signatures, data colouring and watermarking, data anonymization and data obfuscation

[iii] generally comprises inventions for protecting the cloud from various attacks, such as denial-of-service, flooding, malware, ransomware, account phishing and hijacking etc

[iv] comprises inventions for hypervisor and virtual machines, such as protection from side channel attack, secure virtual machine (VM) migration and VM image hardening

[v] refers to inventions related to security policy/rule specification, enforcement, measure, monitoring, evaluation and audit



Worldwide patent publication trends revealed identity & access management and data security as the two major aspects of cloud security, jointly accounting for about 80% of all inventions over the last decade. In particular, identity & access management, and data security-related security issues, such as data breach, insecure API and insufficient identity & access management, have been identified as top threats to be dealt with in recent years.[11-14] As such, innovation interest in these two aspects is expected to continue in the next 3-5 years.

Network security solutions have registered the highest growth rate amongst the different aspects of cloud security. This recent growing interest is not surprising. Due to the increasing deployment of cloud services across a rising number of industries including finance, healthcare and social media,[1,2,15] new modes of attacks targeting cloud networks have been on the rise in recent years. From a single attack mode, i.e. account, service & traffic hijacking, identified as a top threat in 2010, the modes of cloud network attack have increased to four in the recent 2-3 years, i.e. system and application vulnerabilities, account hijacking, advanced persistent threats (APTs) and denial-of-service (DOS). In particular, inventions related to tackling DOS attacks garnered high interest, growing at an annual rate of 24.8% in the recent 5 years. This is in line with market views that DOS attacks are a major form of attack in cloud computing.[16-19] With a relatively lower number of inventions and the increasing importance of this area, it is important for industry players to keep watch of innovations in this particular aspect of network security.

U.S. AND CHINA ENTITIES LEADING INNOVATION IN ALL ASPECTS OF CLOUD SECURITY

Rank	Identity & access management	Data security	Network security	Virtualisation security	Security policy management
1	Microsoft (96)[iv]	Xidian Uni. (80)	Qihoo 360 (22)	Inspur (34)	Inspur (26)
2	Inspur (80)	Inspur (78)	Qizhi (15)	IBM (25)	IBM (21)
3	IBM (70)	IBM (51)	G Cloud (14)	Huawei (18)	Microsoft (19)
4	Oracle (53)	Uni. Of Elect. Sci. &	Xidian Uni. (14)	Chinese Academy	Zscaler (18)
5	Qihoo 360 (48)	Microsoft (38)	Microsoft (14)	Dell EMC (12)	G Cloud (17)
6	Huawei (48)	Zhengzhou Yunhai (31)	IBM (14)	Microsoft (11)	State Grid Corporation Of China (17)

[iv]Number in parenthesis indicate the portfolio of inventions of the respective applicants

With U.S. and China being the most important markets, it comes as no surprise that top players innovating in the various aspects of cloud security are mainly U.S. and China entities.

Leading U.S. players comprise of commercial entities who are well-established providers of cloud services. In particular, IBM and Microsoft are two top players that have been actively innovating in all five aspects of cloud security. Their capabilities are demonstrated in their commercial solutions, including IBM® Security Solutions,[20] Microsoft Office 365, Microsoft Azure, Windows Server Hyper-V and Microsoft Dynamics CRM.[21]

Chinese leading players comprise a mix of commercial entities and institutes of higher learning (IHLs). In response to government policies towards cloud adoption, IHLs in China are taking steps to align their institutional research to government policies. One of the top commercial players from China, Inspur, has built an impressive technology portfolio with expertise spanning across four aspects of cloud security as it strives towards becoming a leading cloud service provider.[22]

VIRTUALISATION SECURITY A CRITICAL SECURITY COMPONENT TO IAAS SERVICE MODEL

Software as a Service (SaaS), Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) are three of the fastest growing revenue segments of cloud service models[23]. Therefore, it is critical to understand the various security needs of these three cloud service models.

The co-occurrence of inventions relating to virtualisation security and IaaS service model is extremely strong - an astounding 94% of inventions relating to the deployment of virtualisation security lies in the IaaS service model. This innovation interest correlates well with market sentiments where deployment of virtualisation security within an IaaS model is a critical concern in the industry[24-26].

	SaaS	IaaS	PaaS
Identity & access management	208 (78%)[vii]	119/45%	138/52%
Data security	113 (76%)	81/54%	77/52%
Network security	20 (49%)	24/59%	13/32%
Virtualisation security	15/21%	66/94%	12/17%
Security policy management	56 (54.4%)	69/67%	42/41%

[vii] The co-occurrence table shows the number of inventions that concurrently relate to one of the cloud service models and an aspect of cloud security. For example, 208 refers to the number of inventions that relate to both SaaS and identity & access management. The number in parenthesis refers to the percentage of documents relating to a specific cloud service model within inventions that cover cloud service models and a particular aspect of cloud security.

In addition to a low number of inventions in the virtualisation security/IaaS space, this space is fragmented with no dominant player. While SaaS-based cloud computing platform has been the dominant service platform till date, the global market adoption of IaaS is expected to exceed SaaS by 2020,[7] with market penetration of more than 78%,[27] and an estimated market size of USD 150.7 billion by 2023. As such, the IaaS market is primed for further growth in the coming years. These factors point to the virtualisation security/IaaS space as an area to keep a watch over, given the imminent shift into IaaS service models.

Top Applicant for virtualisation security/IaaS	Number of inventions
CISCO TECHNOLOGY	3
VMWARE	3
DELL	3

CONCLUSION

Cloud security challenges abound in view of the rapid adoption of cloud computing platforms. To ensure a safe environment that protects both the service provider and end user, it is crucial for cloud adopters to understand critical issues and threats that bundle themselves with the deployment of cloud services. More significantly, to stay ahead of the security issues associated with cloud computing, it is imperative that innovators are aware of the technology gaps in the current cloud security technology landscape, so as to aptly provide targeted enhanced solutions to tackle security issues associated with cloud computing.

REFERENCES

1. Business Insider US, "The 21 scariest data breaches of 2018", [Online]. Available: https://www.businessinsider.sg/data-hacks-breaches-biggest-of-2018-2018-12/?r=US&IR=T
2. TechWorld, "The most infamous data breaches", [Online]. Available: https://www.techworld.com/security/uks-most-infamous-data-breaches-3604586/
3. IBM, "2018 Cost of a data breach study: global overview", [Online]. Available: https://databreachcalculator.mybluemix.net/assets/2018_Global_Cost_of_a_Data_Breach_Report.pdf
4. Securityweek, "Data breach cost Marriott $28 million so far", [Online]. Available: https://www.securityweek.com/data-breach-cost-marriott-28-million-so-far
5. Verizon, "2019 Data breach investigations report", [Online]. Available: https://enterprise.verizon.com/en-sg/resources/reports/dbir/
6. ABNewsWire, "Cloud security market 2018 applications, development history, leading growth drivers, emerging audience, segments, key vendors analysis and upcoming opportunities - 2023", [Online]. Available: http://www.abnewswire.com/pressreleases/cloud-security-market-2018-applications-development-history-leading-growth-drivers-emerging-audience-segments-key-vendors-analysis-and-upcoming-opportunities-2023_304242.html
7. McKinsey, "Public cloud in China: Big challenges, big upside", [Online]. Available: https://www.mckinsey.com/industries/high-tech/our-insights/public-cloud-in-china-big-challenges-big-upside
8. McKinsey, "Public cloud in China: big challenges, big upside", [Online]. Available: https://www.mckinsey.com/industries/high-tech/our-insights/public-cloud-in-china-big-challenges-big-upside
9. South China Morning Post, "Alibaba says it is on track to overtake Amazon as world's top cloud computing services firm", [Online]. Available: https://www.scmp.com/tech/enterprises/article/2114965/alibaba-says-it-track-overtake-amazon-worlds-top-cloud-computing
10. GeekWire, "Building a wall around the cloud: Why China will soon be a very important cloud computing market", [Online], Available: https://www.geekwire.com/2019/building-wall-around-cloud-china-will-soon-important-cloud-computing-market/
11. Cloud Security Alliance (CSA), "Top threats to cloud computing v1.0", [Online]. Available: https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf
12. CSA, "The notorious nine cloud computing top threats in 2013", [Online]. Available: https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf
13. CSA, "The treacherous 12 top threats to cloud computing + industry insights", [Online]. Available: https://downloads.cloudsecurityalliance.org/assets/research/top-threats/treacherous-12-top-threats.pdf
14. CISION, "CSA releases top threats to cloud computing: deep dive", [Online]. Available: https://www.prnewswire.com/news-releases/csa-releases-top-threats-to-cloud-computing-deep-dive-300693803.html
15. Digitalguardian, "The top 10 finserv data breaches", [Online]. Available: https://digitalguardian.com/blog/top-10-finserv-data-breaches
16. M. Darwish et al., "Cloud-based DDoS attack and defences", *IEEE International Conference on Information Society (i-Society 2013)*
17. InformationAge, "DDos attack volumes increase by 110% in Q3 2018, according to Link11s new report", [Online]. Available: https://www.information-age.com/link11-ddos-attacks-123476662/
18. ITPRo, "DDos attacks increase 40% year-on-year", [Online]. Available: https://www.itpro.co.uk/security/27808/ddos-attacks-increase-40-year-on-year
19. Betanews, "Public cloud services used to boost DDoS attacks", [Online]. Available: https://betanews.com/2018/09/11/public-cloud-boost-ddos/
20. IBM Security, [Online]. Available: https://www-03.ibm.com/press/us/en/presskit/33537.wss
21. NewHorizons, "Microsoft cloud technologies", [Online]. Available: https://www.newhorizons.ae/training-certifications/cloud-technologies/microsoft-cloud-technologies/
22. DCD, "Inspur cloud aims to reach $3 billion in annual sales by 2020", [Online]. Available: https://www.datacenterdynamics.com/news/inspur-cloud-aims-to-reach-3-billion-in-annual-sales-by-2020/
23. Fourquadrant, "Go to market cloud computing research", [Online]. Available: https://www.fourquadrant.com/go-to-market-cloud-computing-research/
24. K. Hashizume et al., "An analysis of security issues for cloud computing", *Journal of Internet Services and Applications*, 2013.
25. KirkpatrickPrice, "Who's responsible for cloud security", [Online]. Available: https://kirkpatrickprice.com/blog/whos-responsible-cloud-security/
26. NetworkWorld, "SaaS, PaaS, and IaaS: a security checklist for cloud models", [Online]. Available: https://www.networkworld.com/article/2199393/saas--paas--and-iaas--a-security-checklist-for-cloud-models.html
27. Frost & Sullivan, "Global cloud infrastructure as a service market outlook, forecast to 2023", [Online].

ABOUT IPOS

The Intellectual Property Office of Singapore (IPOS) is a government agency under the Ministry of Law. We use our intellectual property (IP) expertise and networks to drive Singapore's future growth. Our vision is for a Singapore where innovative enterprises use their IP and intangible assets to grow. More information on IPOS can be found at www.ipos.gov.sg

ABOUT IPOS INTERNATIONAL

IPOS International is a wholly-owned subsidiary of IPOS, offering innovative IP solutions to catalyse enterprise and industry growth. We help companies leverage on their IP and intangible assets through IP strategy and management, patent search and analysis. More Information on IPOS-I can be found on www.iposinternational.com

Contact us

For enquiries, please contact us at ipos_enquiry@ipos.gov.sg.