FROST & SULLIVAN

Cloud-based Identity and Authentication:

BIOMETRICS-AS-A-SERVICE

A White Paper by Frost & Sullivan
in collaboration with Fujitsu

CONTENTS

INTRODUCTION

In today's digital landscape, enterprises and consumers alike are rapidly embracing the shift towards a social and mobile era. As more enterprises adopt a faster, more efficient, "on-the-go" business approach, portable mobile devices such as smartphones, tablets, notebooks are poised to become powerful tools for conducting everyday business transactions for users working in a multi-device and location-independent environment.

The growing use of personal or employee-owned devices for work-related activities is catalyzing the need for enterprises to establish a Bring-Your-Own-Device (BYOD) strategy. Tech-savvy users are driving the proliferation of data-driven devices, apps and sensors and delivery platforms towards cloud and social technologies – enhancing both business and customer communication to make it more seamless and mobile.

Mobility is causing a wave of digital disruptions across many industry verticals mobilizing workforces and presenting tremendous benefits in business segments that employ mobile customer services. While banking, finance, and insurance sectors have been prominent users of portable devices for business; healthcare, retail and e-commerce sectors are expanding their portfolios to include mobile-centric applications and services in anticipation of a more digital-savvy consumer profile.

Emerging technologies are reshaping the financial services ecosystem. With the steep decline in traditional payment methods such as cheque and cash, emerging digital payment technologies are rendering more secure, flexible, and convenient methods for cashless financial transactions. In the banking sector, mobile and online platforms enable banks to use mobility as a multi-faceted tool to drive customer engagement, improve convenience, and create competitive advantages for services such as accounts servicing, investment portfolio, customer services and transactions.

Technology is also changing the way people shop and how retailers operate. The growing impact of mobile devices in the digital landscape is spurring the phenomenal growth of electronic commerce and mobile commerce in the retail market. Retailers are prioritizing investments in e-commerce platforms over conventional in-store IT systems upgrades, as businesses prepare for the anticipated rise in sales from online and mobile shoppers.

Enterprises and service providers are also starting to adopt new mobile strategies for the entire business value chain – from corporate IT, customer engagement right through to customer purchasing patterns. Mobile devices significantly increase worker productivity, improve supply chain operations, ensure agility for more efficient business operations, while facilitating real-time collaboration with customers, partners, and suppliers. Frost & Sullivan believes that organizations leveraging mobility to manage the shift to a "virtual enterprise" framework are likely to see increased efficiencies and operational advantages in their respective industry verticals.

More employees are using their personal mobile devices in mobile banking and mobile commerce to access sensitive personal information as well as payment-related transactions. While BYOD delivers significant advantages in work flexibility and efficiency, it could, however, also attract the threat of cyberattacks due to the lack of security measures like anti-malware software and personal firewall commonly found on personal computers. The use of personal devices for simple work functions escalate the need for data and network protection from malware intrusions as well as lost and compromised devices, all posing serious risks to the enterprise and individual's private information. Protection for enterprise data stored on the employee- or corporate-owned devices is critical for enterprises. According to the Frost and Sullivan Enterprise Survey,

approximately 58% of large enterprises have a formal BYOD policy while only 20% of small businesses have a standard policy.

While businesses strive to implement the right mix of technologies and policies for BYOD, users could increase the risks by exposing themselves to web-based attacks from malicious programs that reside on unprotected sites and devices making their way to either the user's personal space or enterprise environment. With BYOD gaining popularity in businesses across different industries, cyberattacks are likely to become more frequent, sophisticated and capable of targeting a particular segment of population or institution. The constantly-evolving threats, cyber security, operational and legal considerations make it necessary for companies to evaluate how best to implement a business mobility strategy while protecting customer and business data.

COMPLEX THREAT AND CYBERSECURITY LANDSCAPE

The BYOD approach brings numerous benefits to businesses including increased job efficiency and flexibility, IT department cost-savings, greater employee job satisfaction and better response times. However, allowing employees to use their own devices to access company information could also heighten security threats and risks. The growth of online and mobile banking, as well as electronic payments, are prompting service providers, banking, and e-commerce sectors to invest in advanced security measures to prevent criminals from targeting their customers.

The key factors driving cybersecurity demand and its security challenges are:

CLOUD-ENABLED BYOD

With BYOD policies becoming more pervasive across different industries, a cloud-enabled architecture offers a secure, flexible and cost-efficient solution. Innovations in cloud-based applications support the evolving operating environments and organizational workflow with the goal to improve business productivity and efficiencies. The ability to work in a desk-less environment; from being deskbound to mobile presents significant opportunities for innovation by introducing features that are unique to mobility, i.e., location and routes.

CHALLENGES

With more businesses employing cloud applications and mobile devices for mission-critical processes and storing company information in public cloud services, enterprises are at risk of data breaches, fraud and other malicious threats without the proper measures to prevent cyberattacks. By 2016, almost 56% of enterprises are expected to store mission-critical workloads and applications on the public cloud platform (Source: Cisco Global Cloud Index).

VIRTUALIZATION FOR BYOD

Desktop virtualization enables employees to enjoy a similar experience of accessing their workplace, and working anytime, anywhere across a broad range of devices – from desktops, laptops to smartphones and tablets. Desktop virtualization does not only reduce the cost of implementing physical hardware and software and lower maintenance; it enables IT departments to manage operating systems and applications centrally to support access to any device in any location with network connectivity. Desktop virtualization is projected to gain a stronger foothold in the enterprise IT landscape, potentially reducing IT costs while improving employee productivity and business continuity. Virtualization capabilities are referred as to Virtual Desktop Infrastructure (VDI), Hosted Virtual Desktop (HVD), Desktop as a Service (DaaS), and server-based computing.

CHALLENGES

Virtual desktops are susceptible to security challenges similar to physical desktops though the issues are unique to virtual machines. One of the most common threats virtual desktops face is access security. Anyone with access and a password could infiltrate the virtual machine.

EMERGING MOBILE BUSINESS WORKFORCE

The combination of new devices and the ability to use the services anytime, anywhere are being increasingly adopted by business users to perform and streamline business processes and workflows. Frost and Sullivan estimates that a significant number of enterprises in developing economies have 60% of BYOD employed at their workplace (Source: Frost & Sullivan – Desktop Virtualization Whitepaper for Fujitsu). Pervasive collaboration, communications, and social technologies have become business imperatives as a primary platform for engagement and task scheduling. Mobile devices are transforming the corporate workflow for frontline professionals as more business services delivery models move towards business-centric applications in real-time.

CHALLENGES

The influx of IT consumerization fostered by the BYOD trend is not only enabling employees to use their personal devices for work, but changing the way traditional enterprise apps look and operate. As BYOD is increasingly encouraged in the workplace, shadow IT becomes a necessity – and a source of security risk – as tech-savvy employees seek solutions to meet business line problems. Security concerns arise when unsupported hardware or software that are often not in line with the organization's requirements for control, documentation, security and reliability are introduced, resulting in the likelihood of unofficial and uncontrolled data flow. Often when endpoints (applications not network-based) are administered by employees, it becomes complex for businesses to impose security policies. Enterprise decision-makers need to identify these vulnerabilities within the IT department that created the need for shadow IT in the first place.

BANKING AND FINANCIAL SECTOR

Online and mobile financial services have revolutionized brick-and-mortar banking making it greener, faster and more convenient. Banks are adopting secure, flexible methods for customers to access banking services and enhancing the accuracy of identifying customers to boost customer retention and satisfaction. Banks and financial institutions now offer customers more ways to access their accounts, with most services available online either via a web browser or mobile app. However, as online data breaches, transaction fraud, and identity thefts continue to grow, banks are continually looking to improve security beyond username and password protocols.

CHALLENGES

With more than half the global population having access to mobile devices, online banking and mobile banking are becoming common platforms for criminals to target customers. This raises the vulnerability of customer accounts, trust issues, and distress caused to customers prompting banks to look for more robust security measures to detect fraud and prevent cybercriminals from hacking into bank accounts. While online and mobile banking are fast and convenient, they do take away the face-to-face interaction of traditional banking. In addition, banks attempting to strengthen security by relying heavily on passwords and PINs only makes banking inconvenient. What's more these security measures may not be as foolproof as they are also easy to crack.

ONLINE SHOPPING

E-commerce and m-commerce are growing rapidly as a result of changes in consumer buying behavior, access to credit, numerous online and mobile shopping sites along with the proliferation of portable devices and applications. Mobile sales by the 500 leading mobile commerce sites are on pace to reach US$155 billion in 2015, up 68% from US$92.4 billion in 2014, with shopping being the primary driver for e-commerce market growth (Source: Internet Retailer 2016 Mobile 500). E-commerce is changing the way companies do business and consumer buying preferences. Today, businesses can feature a wide range of products online, access a larger customer base and better suppliers as well as expand the business to international markets. Customers can purchase almost anything online 24/7, make quick buying decisions based on user reviews, and enjoy a wide range of payment options, enhancing the consumer shopping experience.

CHALLENGES

In the e-commerce space, fraud and payment card data theft continues to be the top data breaches. According to Frost & Sullivan, an estimated 54% of attacks target e-commerce platforms, with this figure set to dominate the e-commerce landscape in the next few years. A common issue at the root of e-commerce is that the identity of customers making the payment transactions is unknown, as the person making the purchase is on a distant computer. Passwords and PINs can be stolen or used without permission resulting in security and data breaches, loss of customers and increased cost for the industry. E-commerce service providers are increasingly challenged in this perspective and continually exploring options to leverage advanced technology to optimize security for a wider range of transaction types.

Enterprises recognize the ever-evolving threat to the BYOD business space and the growing volume of cyberattacks. Critical measures are required to protect sensitive business and personal data as well as to safeguard national security. In a global report, the incidence of security attacks reported in 2014 have risen to 42.8 million; an increase of 48% from 28.9 million in 2013 (PWC, Global State of Information Security Report). With the rising incidence of fraud and data breaches, customers are looking for safer ways to make purchases via online and mobile payments. As enterprises look to address the growing complexity of IT security, it is imperative that more businesses adopt new and higher levels of security compared to the traditional security systems such as Identity and Access Management (I&AM) systems.

Challenges facing I&AM and complex IT security issues include:

HAVING A DIVERSE NUMBER OF DEVICES AND OPERATING SYSTEMS	The proliferation of mobile apps and a mobile business workforce result in the escalated availability of more devices and services to be managed with diverse requirements resulting in greater IT management for end-user segments to appropriate devices, services and access.
DIFFICULTY MANAGING IDENTITY AND ACCESS IN THE WORKPLACE	It is increasingly difficult keeping track of employees as their roles change, and access to work information remains unrevoked, although it is no longer required. To ensure that access is granted to role-specific employees, businesses need to spend time mapping information from disparate systems into human resources data. ○ Duplication of identity information is often performed on multiple systems such as addresses, phone numbers and employee's basic profile. When identity data is duplicated, there is often a lack of consistency in data updates that are stored and managed independently of each other. ○ In traditional IT organizations, companies delegate systems administrators to perform administrative tasks including providing management access control according to the employee's role requirements. However, issues between the human administration and the monitoring system could occur in the I&AM environment such as: › Cloning of accounts – employees in similar roles being granted the same access level. › Orphan accounts – existing accounts appearing in the system that do not have a clear owner. › Combination of access – employees are given access to certain work sites, but when combined with other granted access can increase security risks.

The Identity and Access Management (I&AM) system serves to provide security to support access management. Featured capabilities are often program-based deployment, entitlement management focused and all user identity management with moderate cost and benefit outcomes. The hallmark of I&AM previously often focused on the provisioning of technology with organizations struggling to meet compliance for effective and secure adoption.

With more people accessing sensitive information while engaging in business-centric workloads, enterprise IT requires to consistently update critical information, security processes and new technologies to prevent losses from security attacks. Mitigating the security risks, especially as more processes move into the digital space, is driving the need for increased data and information security.

THE RISE OF BIOMETRICS

"Biometrics refers to unique identifiers that provide access and control for applications and devices via the measurement of human physical or behavioral attributes."

FROST AND SULLIVAN, 2015

Biometric identifiers are categorized into two distinct types: physiological and behavioral characteristics. Biometrics technology is an approach to positively identify a person's identity using physiological characteristics including fingerprint, face recognition, palm vein, retina and iris recognition. Behavioral biometrics assesses uniquely identifying and measurable patterns of human traits, including characteristics like voice, gait and typing rhythms. Biometrics input or data is typically processed using an algorithm to identify data-specific points entered into a scanner where biometrics information is translated to match the data points, hence, giving authentication access for the user.

In an increasingly sophisticated digital landscape, the need for data security is growing, as consumers and industries incorporate the use of electronics in almost all facets of life. The propensity of a secure digital environment is largely being propelled by the rising demand for mobile and smart devices, cannibalizing both the enterprise and consumer market. The need for enhanced security authentication leveraging new technology tools offer significant advantages over traditional access controls.

BIOMETRICS TECHNOLOGY BECOMING UBIQUITOUS

Biometrics solutions are gaining momentum in a number of domains creating security measures that are more convenient than in other approaches. Globally, the commercial biometrics market earned revenues of US$1.48 billion in 2012 and is estimated to reach US$6.15 billion in 2019 (Source: Frost & Sullivan). The shift in biometrics technology growth is being fueled by the benefits it offers:

Unique to a single identity. No two people can share the same biometrics data.

Cannot be copied. Biometrics technology ensures authentication is performed on live identities.

Cannot be shared. Unique to the individual's physical characteristics and eliminates duplication.

These features, exclusive to biometrics technology, provides greater security measures for intellectual assets as well as workplace and individual information in comparison to common user authentication including passwords, user IDs, single sign-on and other traditional access management methods. Frost and Sullivan projects the market revenue for fingerprint authentication on mobile devices to increase from US$52.6 million in 2013 to US$396 million in 2019.

Growing awareness of using biometrics for identification is expected to spur greater global commercial markets (biometrics devices and applications), and user adoption as many current applications such as banking, healthcare, immigration and border control and access to buildings require user authentication.

In retail and e-commerce industries, vendors are constantly engaging in new technologies to provide customers with crucial information such as pricing, product information, and reviews. More customers are turning to the benefits of online purchases for fast selection and delivery. Retailers are being challenged by the growing number of mobile payment customers, essentially changing the consumer market. The need to deploy fast and efficient online services that allow mobile payments across all channels is a critical prerequisite to enhance customer experience. The use of biometrics for online and mobile shopping provides a secure and easy to use payment approach, offering a hassle-free customer experience for next-generation mobile shoppers. Drawing from the global commercial market, biometrics-as-a-service should address the following key market requirements as stated by industry stakeholders:

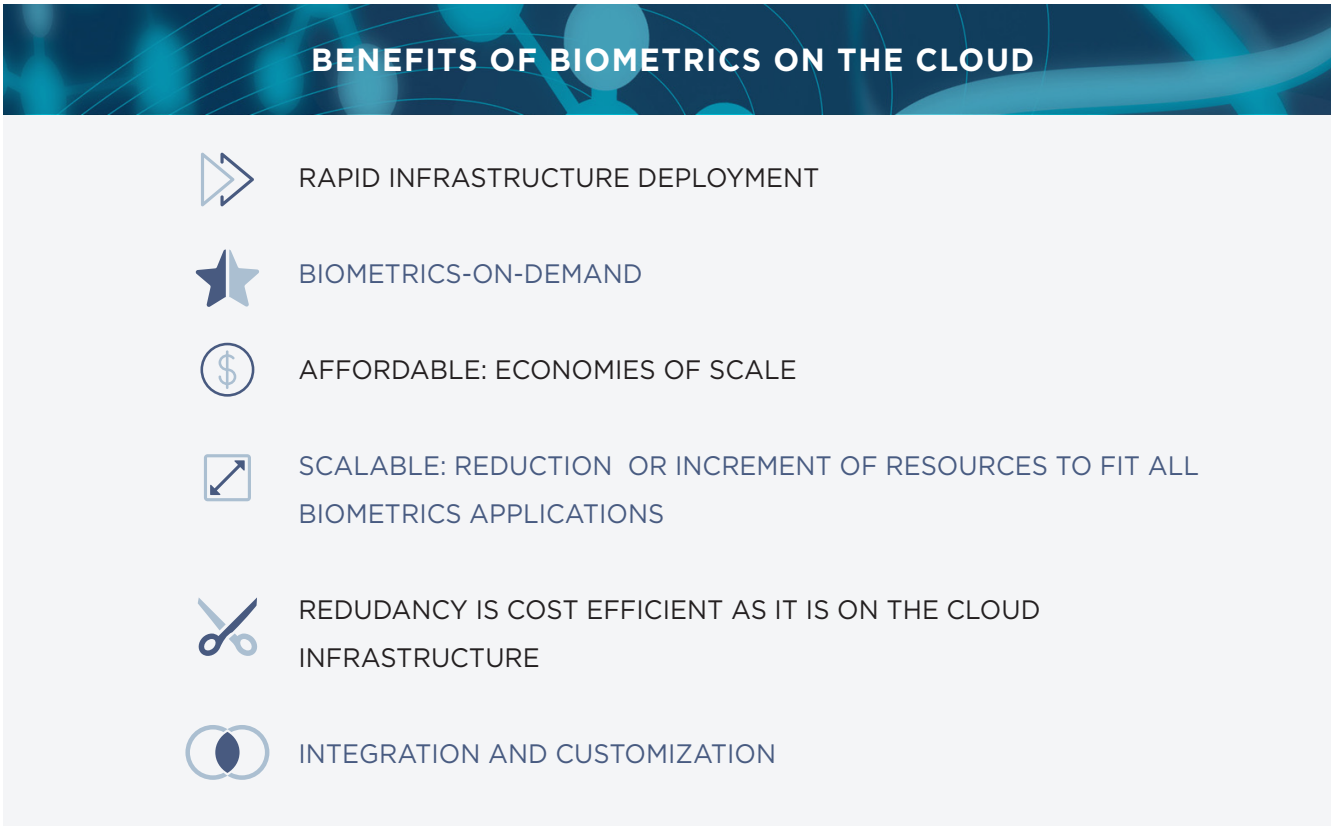
> *"One of the biggest concerns consumers today have is the risk of fraud when shopping online. Savvy cybercriminals are a threat to e-commerce and the online shopping industry diminishing business opportunities in this sector. The top challenge in retail today is to secure the Point of Sale (POS) and omnichannel retailing processes where unified security measures will provide true continuity of customer experience. High-tech biometrics authentication system is the future of secure sales."*
>
> **LEADING E-COMMERCE RETAILERS IN THE US**

TAKING BIOMETRICS TO THE CLOUD

Cloud computing technology marks the next wave of enterprise IT, catering to overall IT consumption and market demands of a digitized economy. The tremendous benefits of cloud technologies are being leveraged by companies of all sizes taking advantage of cloud capabilities including:

- **On-demand environment:** Cloud services can be accessed at anytime, anywhere in the world.
- **Network-centric:** Available on any network connection and device.
- **Economies of scale:** Able to serve multiple customers using a multi-tenant model with different physical or virtual resources that can increase or decrease depending on demand and cost.
- **Rapid elasticity and agility:** Able to swiftly shift and deploy resources across disparate infrastructures.
- **Data sovereignty:** Biometrics over the cloud ensures data sovereignty, which is an important requirement for a growing number of organizations.

Figure 1: Characteristics of the Cloud-Enabled Biometrics



Source: Frost & Sullivan

Taking biometrics to the cloud enables cloud-enhanced capabilities and technologies to be assimilated on the entire biometrics infrastructure of a service provider. Infrastructure includes virtual servers incorporating biometrics template databases, networking and storage components and other types of automation and processing required to verify and identify transactions. The only hardware component the host or service provider requires is to purchase or develop a biometrics capture device (i.e., retina and fingerprint scanner, or vein pattern recognition device). A biometrics business hosted on a cloud-based model supports a wide range of biometrics applications and technologies.

Figure 2: Differences between Cloud-based I&AM and Conventional On-Device Solutions

CLOUD-BASED I&AM SOLUTION

- Cost-savings via automation.
- Universal access across all applications and devices.
- Auto back-up of data.
- Integration with internal directory and external services.
- Single-sign-on.
- Flexible multimodal solution secures all access channels.

ON-DEVICE SOLUTION

- Costly to implement different types of endpoints.
- Lacks centralized capabilities to manage data on different devices.
- Relies on end-user to complete data back-up on mobile devices.
- Inability to integrate and interoperate.
- Weak in defending threats.
- Secures only one access channel.

Source: Frost & Sullivan

BIOMETRICS MEETS BANKING

As banks become more digitized, cloud computing can provide benefits including reductions in administrative and operational expenditure through automation and optimization of IT resources. With the growing interest in providing customers with enhanced banking security and cutting-edge technology, biometrics can identify a person as opposed to just identifying a piece of information or device. Biometrics can never be forgotten or shared with others. Also, biometrics data is difficult to steal as long as the biometrics vendor uses the appropriate architecture and security methods. Major banks leverage biometrics technologies in a variety of scenarios including cash withdrawals at the ATM, authenticating mobile banking apps using fingerprint sign-in or a combination of face and voice verification. Classified banking information can also be hosted by one cloud service provider while the bank's security biometrics infrastructure including its biometrics system can be outsourced to the cloud making it scalable to meet the growing demands of customer security needs.

Case Study: Banking with Biometrics

STEP 1	• Login to an online banking website using a PC. • Login to a mobile banking app using a mobile device (iOS or Android).
STEP 2	• Verify a banking transaction from a banking website. • Verify a banking transaction from a mobile banking app.
STEP 3	• Verify a transaction performed at an ATM, by using GoVerifyID®. • Detect and prevent fraud by authorizing/declining unusual transactions through biometrics authentication. • Authorize periodic charges/payments (credit card payments, service payments).

SECURE PAYMENTS – THE NEXT FRONTIER

The e-commerce and m-commerce segments are poised to rapidly accelerate with the adoption of cloud biometrics for authentication with built-in biometrics support (especially for smartphones) to prevent rising identity theft and payment fraud. A system for verifying the buyer's identity is the next cutting-edge technology in the fraud fight.

FIDO (FAST IDENTITY ONLINE) is a universal open-based approach that introduces two-factor authentication and standardizes password replacement. The FIDO standards support multifactor authentication (MFA) as well as other authentication methods including biometrics, Near Field Communication (NFC), USB security tokens, among others to replace the need for a password.

Established by an alliance of industry heavyweights, including Paypal, Lenovo and Microsoft, FIDO addresses the authentication problem using two disciplines: the Universal Authentication Framework

(UAF) that supports user devices with fingerprints or PINs by logging on using a public key; and the Universal 2nd Factor (U2F) that authenticates users with a second factor using a PIN with USB touchscreen key or NFC-enabled mobile device. Apart from the benefits of two-factor authentication, incorporating MFA into devices addresses the standardization issue as interoperability capabilities are reduced by competing standards and have resulted in lower user adoption rates in the payment industry. A better authentication solution in tandem with services, methods and devices that suit the entire business chain is necessary for a biometrics-driven economy.

FUJITSU'S VALUE PROPOSITION AS A BIOMETRICS-AS-A-SERVICE PROVIDER

From the traditional I&AM to the changing biometrics landscape, the biometrics technology now incorporates the new multimodal biometrics using various sensors to capture sets of information from the same marker including multiple image scans from an iris or fingerprint scanning system by a worn-out finger allowing greater accuracy i.e., two or more biometrics, increased reliability recognition and enhanced security.

As a leading ICT services provider, Fujitsu envisions developing a cloud-based biometrics platform that is hardware and algorithm agnostic to match the multifaceted business needs of users. Its new Biometrics-as-a-Service meets the need for holistic end-to-end provisioning of an enterprise grade, cloud-based identity platform through Fujitsu's successful partnership with ImageWare® Systems (IWS).

IWS is a global leader in mobile and cloud-enabled, multimodal biometrics identity management solutions. By leveraging IWS' powerful biometrics authentication technology, Fujitsu's cloud Infrastructure-as-a-Service (IaaS) and Software-as-a-Service (SaaS) prepares enterprises for a BYOD workplace environment and security-enhanced services for mobile transactions.

GoCloudID® is at the heart of IWS' cloud-based biometrics management and identification services. IWS' GoCloudID® deployed on Fujitsu's cloud technology enables rapid integration of existing business applications, operating on a pay-as-you-go model with plug-n-play biometrics.

IWS' GoVerifyID is a mobile biometrics authentication application that connects to the GoCloudID® services. It is used to verify a user's identity to grant access to secure physical or digital sites or to protect transactions via mobile devices. Users enroll their face and voice biometrics as a password replacement. GoVerifyID works with the IWS GoCloudID®'s secure application server layer, GoMobile Interactive®. Its biometric storage service delivers fast, accurate identity verification to protect important applications, systems, and data such as:

- Corporate systems
- Bank accounts
- Financial transactions
- Healthcare records

GoVerifyID and GoMobile Interactive® are designed to work seamlessly with IWS' technology portfolio, including complex biometrics data encryption, persistence accelerators, and patented identity management configurations. GoVerifyID is secure, simple to use, and designed to provide instant identity verification by

engaging with the biometrics capture capabilities of each user's mobile device, allowing it to:

- Create a baseline biometrics enrollment profile.
- Store a user's biometrics data in the cloud.
- Perform biometrics verification of a user's identity against their enrolled profile.
- Send customized messages to users.
- Perform two-way messaging communications.

When the GoVerifyID application captures a user's biometrics, it is transmitted to IWS' GoCloudID® platform, converted into digital biometrics templates, and stored anonymously via Fujitsu's cloud-based, Software-as-a-Service (SaaS) system.

Figure 3: Unique Characteristics of ImageWare® Systems' GoVerifyID Biometrics in the Cloud

SECURE	SCALABLE	ADAPTABLE
Personal, Accurate, Anonymous	***Speed, Population, Device***	***Multi-Biometric, Fusion, Situational***
• Identifies the person not the device • Multi-layer protection of individual user's biometric data • Fast, accurate, and anonymous authentication	• Operates at the speed of business (real-time identify verification) • Scales to hundreds of millions of identities • Cloud-baseed matching, register once use anywhere	• Supports any kind of biometric - single or multiple • High-assurance multi-biometric fusion • Broad applicability for nearly any use case

Source: ImageWare System

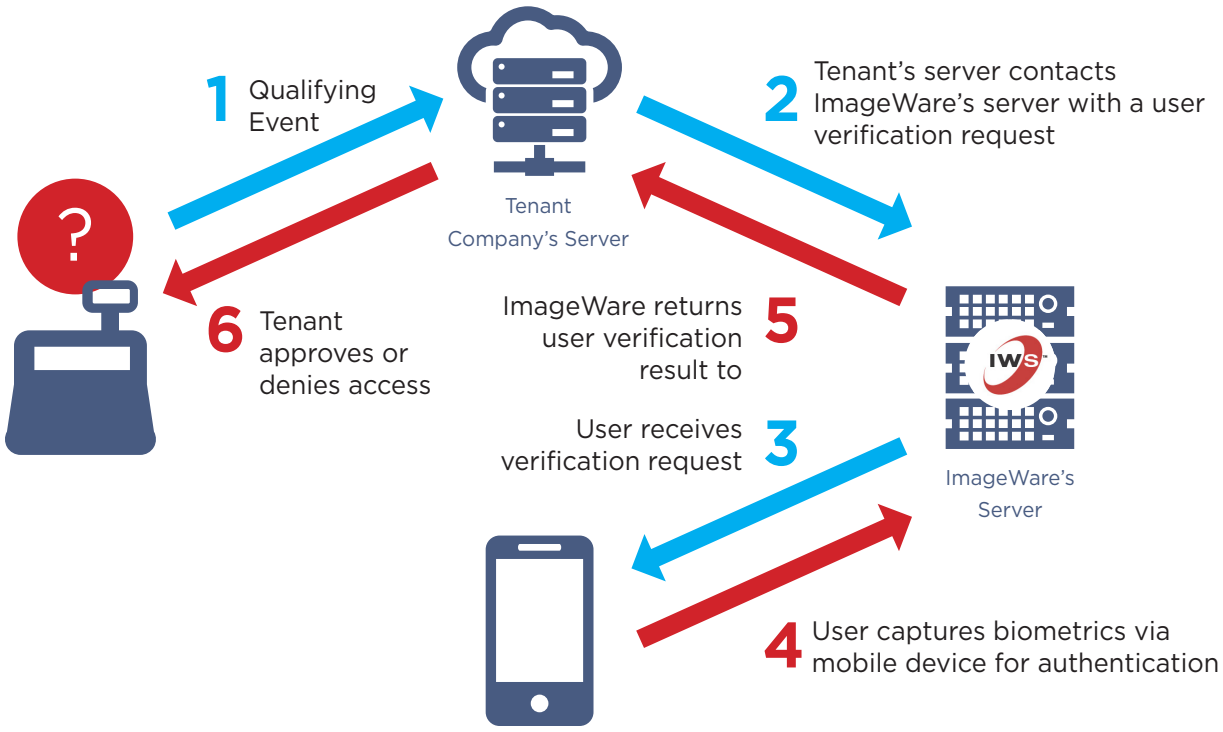
SECURE

Personal, Accurate, and Anonymous

- Biometrics-based authentication uses an individual's physical traits to verify his or her identity. It is like your own personal password that cannot be forgotten, lost, or stolen. Users no longer need to remember the answers to security questions, nor do they need to carry a separate single-purpose hardware token. Biometrics data is intrinsically connected to a person. It is the "What the person 'is' factor" (biometrics), versus a "what a person 'has' factor" (e.g., token or phone), versus a "What a person 'knows' factor" (e.g., password, PIN). It cannot be forgotten or easily compromised.
- All aspects of the IWS solution are fully secure and protected with end-to-end encryption of users' biometrics data.
- Secure Storage is available via the leading Trusted Public Cloud Service Providers (AWS, Fujitsu, or your preferred cloud). Anonymous storage of biometrics data means that even if the biometrics data is compromised it cannot be associated with a person – so it does not provide any value to a hacker.

SCALABLE ***Speed, Population, and Device***	○ Highly-scalable biometrics engine that has the ability to process hundreds of millions of transactions in real-time. ○ Large scale to support hundreds of millions of user identities and transactions with high accuracy and interoperability of different modalities. ○ Cloud-based matching allows a single enrollment of biometrics data to be used on any device, ensuring data integrity, consistency, and availability.
ADAPTABLE ***Multi-Biometric Fusion, Agnostic, In-Band and Out-of-Band Authentication***	○ Patented multi-biometrics fusion provides the industry's highest level of identity matching assurance. ○ The IWS solution is biometrics algorithm agnostic. It supports a wide range of vendor algorithms, including singular or any combination of features including face, voice, iris, fingerprint, palm or vein. ○ It is hardware agnostic supporting a broad range of vendors' hardware device readers including cameras for face and/or iris, fingerprint scanners, palm scanners, vein scanners, audio devices; and available on both Android and iOS systems. ○ Broad applicability across nearly any use cases for both in-band and out-of-band authentication workflows.

Figure 4: ImageWare® Systems' GoVerifyID Solution Workflow



Source: ImageWare Systems

Figure 5: Use Cases and Challenges

FUJITSU USE CASES

HEALTHCARE CHALLENGES	FUJITSU BIOMETRICS-AS-A-SERVICE SOLUTION
• **The healthcare industry** recognizes the need to store and access patient information via secure channels to ensure high confidentiality of patient data and information. • Hospitals are moving away from password authentication as it is not secure. • Establish secure patient identification in the system. • Eliminate health fraud, duplicate medical records and raise safety levels for patient and staff.	• Hospital staff able to access the patient's electronic health records or Personal Health information. • Doctors or nurses can share patient records with other staff using the same system. • Enables remote access allowing doctors to access patient information from mobile devices and mobile health services. • Patient check-in uses biometrics to accurately identify the patient.

BANKING CHALLENGES	FUJITSU BIOMETRICS-AS-A-SERVICE SOLUTION
• **The banking industry** recognizes the need for highly secure identification verification to prevent security breaches and transaction fraud. • Banking areas that are at risk include the ATM, online transactions, branch banking, mobile banking, and single sign-on for bank network security. • Need to improve customer trust to enhance branding and mobile banking applications including mobile payments.	• Login to online banking via PC or mobile device and verify transactions from web-based banking site or mobile banking app. • IWS's GoVerifyID verifies transactions on ATM, mobile banking, online banking. • Verification through biometrics authentication of fraud prevention by authorization or decline of unusual transaction.

Source: Fujitsu

MARKET CHALLENGES WITH BIOMETRICS

As connectivity continues to drive enterprise mobility, the amount of associated personal and public data is set to grow exponentially. Users are increasingly providing their online identities to fulfill demand from organizations to gather, sort and analyze data for valuable insights. Privacy is a significant concern among individuals using biometrics for identification. Biometrics presents certain unique challenges that might not arise from conventional methods such as password or paper documents. For example, facial characteristics can be easily captured without an individual knowing that they are being photographed. Likewise, fingerprints can also be collected (or stolen) because people leave latent prints when touching hard surfaces. Another

privacy concern is when biometrics identification data is captured and used for a different purpose without the person's consent or knowledge. This is especially relevant in security activities conducted by government agencies where individuals' biometrics are matched against future samples or situations (i.e., cross-matching of fingerprints for police to track down suspects). Another concern arises from the biometrics characteristics (e.g., from iris images or wearing down of fingerprints) that may divulge secondary data about an individual's health, occupation or socioeconomic status. Consequently, the person's wish to maintain anonymity in a particular situation may be denied their privacy by biometrics recognition.

Biometrics has a challenge that is inherently device-dependent. Almost all biometrics features and applications required is device-specific for individuals to get access to their sensitive information.

Another challenge for biometrics users and solutions carriers is that because of the multi-party system, the need to establish a biometrics propriety solution can diminish especially when there are more than two or three parties in the same working environment process. There are different users with varying roles, access needs, devices, and mobile device management profiles that are not controlled by the carrier. This could reduce standardization in working processes and policies, and decrease productivity due to lack of collaboration, resulting in poorer company performance. Hence, new policy and biometrics security enhancement measures beyond devices are extremely important and essential for the future cybersecurity landscape.

FUTURE OUTLOOK

The government sector including border control, national identification and law enforcement agencies have been early adopters of biometrics. With the growing proliferation of mobile devices in the enterprise landscape, Frost and Sullivan expects to see growing demand for biometrics applications for identity authentication and online transactions across multiple industries.

High-risk industries such as the banking sector are investing heavily in biometrics. In 2015, banks and financial institutions spent approximately US$350 million on voice biometrics, with spending likely to double to US$700 million by 2019. Biometrics is also expected to be widely adopted in the insurance industry over the next few years to manage the complex ecosystem of carriers, agents, brokers and advisors. Globally, it is estimated that about 70% to 80% of mid-size insurance companies already adopt a BYOD strategy. As a result, future spending in the insurance business is expected to target mobility solutions, security and enterprise apps. The need for highly-secure biometrics identification and verification in managing risk, recruiting and retaining customers and other health insurance provisioning across the insurance business landscape is imminent.

"The insurance business these days is geared towards providing on the door customer experience and services. Captive and geographically dispersed agents and brokers are mobilized, improving sales rates, customer visibility and productivity by embracing BYOD. Biometrics for verification offers convenience for agents and customers for high levels of security access for insurance policies and transactions."

LEADING INSURANCE COMPANY FROM AUSTRALIA

The application of biometrics for identification is likely to expand across markets led by convergence trends affecting biometrics technology providers, ICT networks, security and cloud storage industries, at-risk verticals such as banking, healthcare, and retail as well as OEMs and device manufacturers including smartphone makers. Apple was among the first to incorporate fingerprint identification on its phones which has since become a must-have feature other smartphones must match. Chinese OEMs are also looking to manufacture smartphones by partnering with local suppliers for both camera and biometrics fingerprint-recognition features. Fujitsu will drive the biometric landscape further by developing new systems including encrypting biometric data on features like finger prints and iris scanner that will potentially be the major security tool for the biometric industry.

FROST & SULLIVAN

WE ACCELERATE GROWTH

WWW.FROST.COM

Auckland	Colombo	London	Paris	Singapore
Bahrain	Detroit	Manhattan	Pune	Sophia Antipolis
Bangkok	Dubai	Mexico City	Rockville Centre	Sydney
Beijing	Frankfurt	Miami	San Antonio	Taipei
Bengaluru	Iskandar, Johor Bahru	Milan	Sao Paulo	Tel Aviv
Bogota	Istanbul	Mumbai	Seoul	Tokyo
Buenos Aires	Jakarta	Moscow	Shanghai	Toronto
Cape Town	Kolkata	New Delhi	Shenzhen	Warsaw
Chennai	Kuala Lumpur	Oxford	Silicon Valley	Washington D.C.

ABOUT FROST & SULLIVAN

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies?

Contact us: Start the discussion

GLOBAL

877.GoFrost myfrost@frost.com

APAC

(65) 6890 0999 apacfrost@frost.com