Identity And Access Management – Future Trends

A robust IAM (Identity and Access Management) solution has become an integral part of enterprise IT. A secure, flexible, and adaptive Identity & Access Management (IAM) solutions will enable organizations to improve employee’s productivity and boost their overall security features. Identity & Access Management is no longer limited to controlling access to a system or resource. Access control now also be applying to networks, internet connections, websites, printers, server rooms, software applications, Wi-Fi and many more. In the recent past, we have seen a tremendous growth in technologies like IoT, Big Data, Cloud Computing, and BYOD. IT Security has obviously become a hot topic as each of these technologies depend on it, and with an increasing number of threats, Data Security has always been a prime concern. Limiting access to data and information according to their work requirement for the users helps to reduce the risk of data leakage. With the advancement in technology and identity environment, it has become a challenge for the IT Security to manage with the traditional approach. IT leaders are required to develop their identity and access management (IAM) strategies, and the solution providers need to come up with new features & innovation.

Traditional IAM will have to be armed to deliver on modern day expectations, we will discuss how in future IAM will shape keeping on going innovations and disruption in mind like IOT, Cloud, Blockchain, AI and ML.

IAM & IoT

IAM & Cloud

IAM & Blockchain

Artificial Intelligence (AI) & Machine Learning (ML)

Customer Identity & Access Management

Comparing Traditional IAM, IoT IAM & Blockchain IAM

Key Difference

Bring Your Own Device (BYOD)

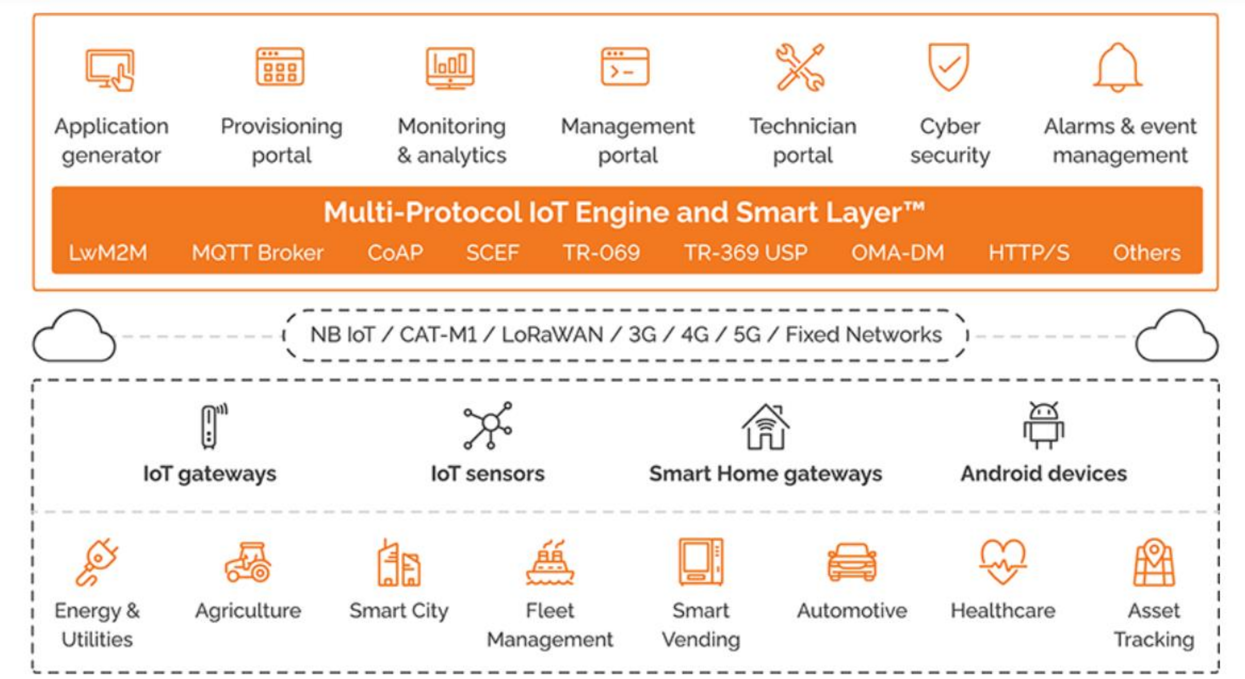
Conclusion

In the near future, organizations will look for below five innovations in Identity & Access Management (IAM) solution:

IAM & IoT

The growing emphasis on digital transformation is encouraging more organizations to adopt initiatives driven by the Internet of Things (IoT).

As our world becomes more connected, it also becomes more complex. Especially when it comes to identity and access management (IAM). This is a challenge that impacts us all, from the individuals accessing services to the enterprises and operators whose role is to authenticate and authorize individuals and devices accessing the internet every day.



Identifying users and things

Mobility is the key to new services and enabling new revenue streams. That means digital identity solutions across mobile, federated or IAM cloudbased platforms are crucial for individuals and services. Why? Because they counter-act the growing issue of identity exposure and unexpected digital threats. When it comes to personalized services, issues of identity validation, consent, attribute sharing, and trust management really matter. This need for resilient, advanced IAM spans across IoT devices, individuals and services, from internet banking to smart metering. Some may need more security than others: internet banking, for example, will need the highest security multi-factor authentication (MFA), consent and authorization. With many IoT devices' service life spanning decades, having the right mix of algorithms and key sizes for the authentication, authorization and encryption protocols is a must.

Implementing security for identities from the start

When it comes to launching a new service or introducing an entire fleet of connected IoT devices (such as smart meters) the challenge is the same: ensuring security is tight from the very beginning. Success lies in creating future-proof, secure IAM solutions that, in turn, become business solutions.

Ericsson have a leading position in digital identity, IAM, cloud and now analytics and security management products. By bringing these together in our ground-breaking digital identity management solutions, we can prevent breaches of security.

It starts with the right building blocks. Technologies such as PKI, GBA, Blockchain, OAuth, OpenId Connect and e-SIM management offer the foundations for a complete, user-friendly, automated and secure authentication and authorization solution.

Cross-domain identity of things

The rapid expansion of the Internet of Things (IoT) calls for a clearer common understanding of how identities function in the digital world. With IoT made up of an endless number of domains, the next challenge is how to manage the single and overlapping identities that come from them. The key? Being able to manage these multiple identities across different domains efficiently by employing the cross-domain identity management solution that best meets its specific requirements.

IAM & Cloud

It can be difficult for a company to start using cloud Identity and Access Management solutions because they don’t directly increase profitability, and it is hard for a company to cede control over infrastructure. However, there are several perks that make using an IAM solution very valuable, such as the following:

- The ability to spend less on enterprise security by relying on the centralized trust model to deal with Identity Management across third-party and own applications.
- It enables your users to work from any location and any device.
- You can give them access to all your applications using just one set of credentials through Single Sign-On.
- You can protect your sensitive data and apps: Add extra layers of security to your mission-critical apps using Multifactor Authentication.
- It helps maintain compliance of processes and procedures. A typical problem is that permissions are granted based on employees’ needs and tasks, and not

revoked when they are no longer necessary, thus creating users with lots of unnecessary privileges.

IAM & Blockchain

Blockchain has proved itself to be tamper resistant and secure. It is increasingly getting attention from companies changing from centralized to decentralized systems. This paper proposes a system for identity and access management using blockchain technology to support authentication and authorization of entities in a digital system. A prototype demonstrates the application of blockchain in identity and access management using the Hyperledger Fabric framework. It provides a proof of concept based on a use case concerning Electronic Health Records from the healthcare domain where an immutable and auditable history is desired for data concerning patients. Basic authentication and authorization operations are able to execute in 2-3 seconds with an initial size of blockchain of about 3.8 MB covering physicians in Denmark.

Decentralized identity is how individuals control when, where and with whom they share their credentials. In the physical world, we take this sharing of credentials for granted – yet a secure, smart way to do this has been long missing in the digital world.

Artificial Intelligence (AI) & Machine Learning (ML)

From Machine Learning to natural language processing, Artificial Intelligence and cognitive computing are elevating beyond speech recognition and rule-based systems to help organization consume and derive value from big data and drive decision-making through powerful analytics.

Artificial intelligence (AI) programming algorithms can be used to data-mine, and the technology like Big Data can reveal the suitable data patterns as part of the data analytics. Many Banking systems are already using this type of analysis globally to reduce fraud. A Machine-Learning system based on Artificial Intelligence, can get to know a person incredibly well such that all the research and data collected about them, combined with multi-factor authentication, will securely identify most people.

The powerful method of IAM access patterns is the Behavioural analysis which can bring policy violations to the surface. The combine efforts of Artificial Intelligence (AI) and Machine Learning (ML) explicitly used to alert on behavioural changes in application and user. These changes could include the API client (e.g. web console vs Python Boto), the location of the API call (e.g. the US vs Europe), or the types of permissions. Analytics combined with artificial intelligence will offer focus and discourse insights so each technical and non-technical worker will work longer and economical.

IAM solution provider will require to build expertise to control the security concerns for Public Cloud Services like AWS, Azure and GCP. In an organization, if you are using hundreds of services from a Cloud provider, it may get difficult to understand who/what has access to which resources. This is challenging, but the IAM solutions, policies, approach, and capabilities are continuously growing. However, in addition to standard IAM issues, organizations are facing few Cloud-Specific challenges as well like Orphan SaaS accounts, multiple admin accounts and users bypassing organization IAM controls which reflects a lack of control over the account lifecycle that many SaaS scenario presents.

To handle these challenges, IAM solutions providers must come up with a better governance strategy for identities. The innovation of new technologies has enhanced the present IAM compliance controls with the help of new insights and automated process. It can detect anomalies and potential threats and does not require an oversized team of security consultants. It helps IAM solution to work in a preventative or even corrective approach of access management, rather working as reactive access management

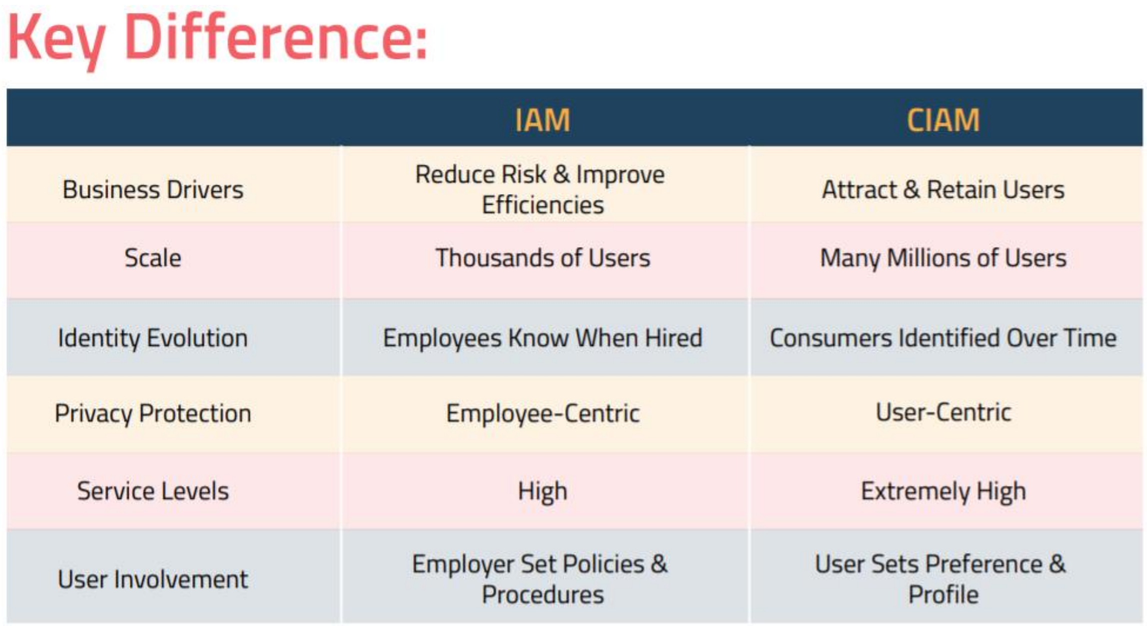
Customer Identity & Access Management

Traditional businesses or the new-age ones, customer has always been every businesses priority. Every organization want to provide the best customer experience, and for this purpose, they request customers to provide valid data and information.

It is a common misconception that technology & approach for consumer identity and access management (CIAM) is the same as that for traditional identity access management (IAM).

Traditional IAM is designed to control employee access to internal data & application. It does not provide insights into who a user is. CIAM platforms, on the other hand, are designed to give companies maximum value from customer profile data and give a better insight into who this user is.

Key Difference



Key Difference:

	IAM	CIAM
Business Drivers	Reduce Risk & Improve Efficiencies	Attract & Retain Users
Scale	Thousands of Users	Many Millions of Users
Identity Evolution	Employees Know When Hired	Consumers Identified Over Time
Privacy Protection	Employee-Centric	User-Centric
Service Levels	High	Extremely High
User Involvement	Employer Set Policies & Procedures	User Sets Preference & Profile

Bring Your Own Device (BYOD)

Many organizations are now adopting BYOD (Bring Your Own Device) approach and allowing their employee partner, customer, and visitors to connect to the corporate network using their own device. This increases the challenge for IT because they need to protect corporate data and yet provide the users with access to the corporate network using their own device. Mobile malware is also threatening security. Thus, it becomes extremely important for Zero-trust security architecture to protect the organisation’s critical assets. Employees, contractors, partners, and others are bringing in personal devices and connecting to the organization’s network for professional and personal purpose, and IT team has no choice to manage or not to manage the devices. The challenge with BYOD approach is not only that outside devices are brought into the corporate network, but also IT need react quickly enough to protect the organization’s data & assets, without disrupting employee productivity and still offering freedom of choice.

Conclusion

Identity access management will continue to evolve in scope and scale. It is very clear that an effective IAM solution should be secure, efficient, simple, productive, compliance, but the cost and complexity involved with deploying a robust IAM solution may delay the process for a most well-intentioned organization as well.
The traditional security perimeter is shrinking. Corporates are searching for IAM solutions with mobile workforce in an organization and a highly distributed and complex network of applications. Identity and access management approach are becoming more complex, and hence the ability to create process & policies based on granular, contextual information will become more and more important.

IAM solutions should be able to make decisions based on various parameters like, user identity, location, device, and the requested resource. And deliver quick access permission to legitimate employees, partners, contractors, or guests—and easily revoke or deny privileges to unauthorized users. Work with IAM solutions that may not yet be perfect, but flexible, governable, and scalable and keeps the future market trends in check.