Classification of IAM Products and Overview of ForgeRock IAM Solution

Mas. Zubair Mulla
Dept. Information Technology
K. J. Somaiya College of Engineering, Vidhavihar
Mumbai-400077, India

Prof. Sangeeta Nagpure
Dept. Information Technology
K. J. Somaiya College of Engineering, Vidhyavihar
Mumbai-400077, India

***Abstract*- Today people around the world are connected through Internet to maintain communication, access and exchange information, contact family and friends. Now-a-days we have gone a step forward to adapt Artificial Intelligence and Internet of Things in our day-to-day life. When world is migrating towards Internet of things then there is a communication between Identities of people and the different electronic gadgets. It becomes mandatory for the organisation to secure Identities while implementing Internet of things so that Identities would not be forged and used to connect to Gadgets. The User Provisioning and Access to different resources play a vital role in this age of connected world. The organisations are adapting to Cloud Computing due to its Service and Delivery Models. It becomes important for the Organisations to not only think about the Data Security but also the User Life Cycle of its employee. The Organisations are taking IT-Security into considerations due to the rising no of Cyber Attacks in this connected world. Identity and Access Management is one of the Pillars of IT-Security. Confidentiality, Integrity and Availability are the prime focus when one thinks of security. When Cloud is used as the service model then organisations have to focus on security to secure the customer data from the outside world. Then Identity and Access Management Solution help them to secure their customer data. Different organisations have different requirements and workflow and thus it becomes difficult for them to get the right solution implemented into their environment. This paper focuses on the different categories of the IAM solutions into the market. This paper also gives an overview of the ForgeRock IAM solution which is Open Source and how it can be beneficial for the organisation in comparison to the various products in the market.**

Keywords: ForgeRock IAM; Internet of Things; Cloud Computing; Artificial Intelligence; IOT

I. INTRODUCTION

The Identity and Access Management Solution is divided into different components like Authentication, Authorization, User Management Life Cycle and Central User Repository. There are various IAM standards proposed over two decades: Lightweight Directory Access Protocol (LDAP), Central Authentication Service (CAS), OZ Protocol, Open Authentication(OAuth), Security Assertion Markup Language(SAML), CoSign Protocol, and OpenID Connect (OIDC)[1].The IAM products utilize anyone of the standards to implement the User Provisioning Life Cycle or Authorization to the Resource.

In this Digital age all the Electronic Devices in the house are connected to the Internet and user handles these devices through Mobile. It is important to secure the Identity of the user as well as connected devices so that it is not misused by the Hacker to gain access into the secured environment. The Effective Identity and Access Management standards should be used to secure Mobile Cloud Computing in the age of Internet of Things. Mobile Devices have become SMART due to the added quotient of Artificial Intelligence. Devices have the ability to track the activities of the user and guess the likes and dislikes of the respective user. Data Analytics is used by the Applications to give solutions to the queries of the users through mobile devices. Information is shared between different applications on the mobile devices. Data on the cloud is the Asset for the organisation to keep it private or public according to the kind of information.

In such a scenario where Information is everything, it becomes mandatory for the organisation to comply with the Confidentiality, Integrity and Availability of the resources. It is the important for the organisation to have Identity Management and Access Management into their Organisation. Identity Management solution will deal with the User Management, Login Management, Role Management, Service Management, Group Management, Policy Management and Workflow Management[2].The Access Management solution will implement the Web Single Sign on Mechanism, Authentication and Authorization framework.

II. CLASSIFICATION OF IAM SOLUTION

The Identity and Access Management system have become an Integral part of the IT industry. The Digital Age is Transforming the way Identities connect with each other. Organisations are also connected through each other and cloud for business purpose. In such a scenario it becomes mandatory for an organisation to choose correct IAM Product. There should be a deep knowledge in the industry about the different types of IAM products available into the industry. In this paper we have tried to explore the different types of products available in the market.

The product selection helps organisation meet the security requirement and also improve the business. The cost effectiveness factor plays a vital role for organisation to invest into the specific IAM Product so that their objective behind implementing the product is fulfilled. Following table represents the different types of products along with the players of the respective product available in the market.

TABLE I CLASSIFICATION OF IAM PRODUCTS

Technologies in the Market	Types of Product			
	Identity Management	Access Management	Privilege Identity Manager (PIM)	Federated Identity Manager
ForgeRock	✓	✓	-	-
Cyber Ark	-	-	✓	-
CA	✓	✓	-	✓
IBM	✓	✓	-	✓

Classification of IAM Products is as follows:

A. Identity Management: This product manages the entire lifecycle of the user information required for Authentication and Authorization. It is also used to manage policies, auditing and user self-service.

B. Access Management: This product provides strong authentication and authorization solution. Access Management is the process of granting access to authorised users. It is used to implement Single sign on mechanism into the organisation.

C. Privilege Identity Manager (PIM): This product is used to assign roles and profiles to the employees of the organisation according to the policies framed. It also keeps a track of all the activities of the user given dedicated roles for Auditing purpose.

D. Federated Identity Manager: FIM [2] provides a simple Identity and Access Management between two organisations with the validation at one organisation and access of the resource at the other organisation so as to avoid cost of deployment and integration of applications into Infrastructure.

III. OVERVIEW OF FORGEROCK IAM SOLUTION

The organisations have to implement different products to fulfil the requirement from the Identity and Access management perspective. The Organisation can use ForgeRock Identity Manager and CA Access manager to complete IAM product. Some organisation can go for a complete package from one technology itself. In this paper we have tried to give a brief overview of the ForgeRock IAM solution by integrating it into the environment as it is open source and easy to be explored as compared to other proprietary products.

A. ForgeRock Identity Management

ForgeRock Identity Management [7], part of the ForgeRock Identity Platform, is an open source projects built from the OpenIDM and OpenICF. This product is designed with a goal to attain identity administration and provisioning solution focused on managing relationships across users, devices and things. This was designed in response to the pain suffered by organizations in deploying legacy enterprise provisioning solutions. The proprietary solutions are mostly monolithic, heavyweight, painfully slow to deploy, and expensive. They are not prepared for today's organizational needs, like connecting to cloud infrastructure and internet-connected devices and things. Unlike legacy identity management solutions, ForgeRock Identity Management is the only 100% commercial open source, lightweight, provisioning solution with scalability. ForgeRock Identity Management is a modular, plug-and-play identity service so you consume only what you need. In addition, it has a well-defined and simple REST API that is ideal for anyone in need of provisioning across enterprise, cloud, social, and mobile environments.

1. ForgeRock IDM Architecture

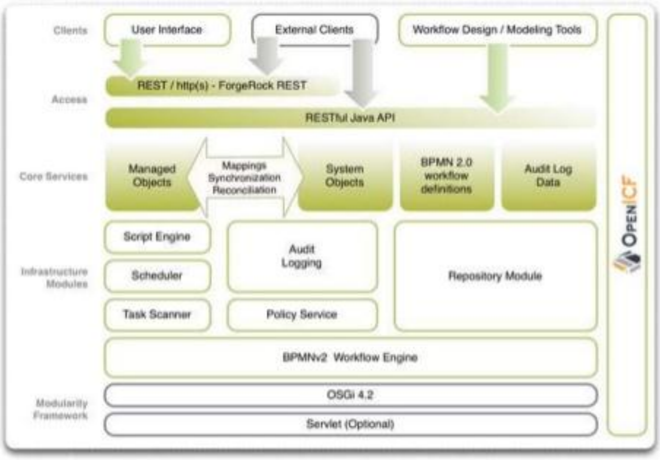

Fig 1. ForgeRock OpenIDM Architecture

ForgeRock IDM is utilizing a Java-based architecture that is built on the OSGi framework and therefore is able to provide lightweight, modular services which are accessible through developer-friendly REST APIs. It is using standard Java development tools such as Eclipse, NetBeans, Spring, etc. This architecture provides multi-layered provisioning activities through an embedded workflow and business process engine based on Activiti and the Business Process Model and Notation (BPMN) 2.0 standard. The modular design enables complete flexibility to use the embedded workflow engine and a database or replace these technologies with your selected platforms and services. The entire service can be completely embedded and custom-tooled to the requirements of the target applications or services. The built in identity framework is used to manage all the identity sources like external systems, databases, directory servers, and thus eliminating the need to rip and replace data stores.

The basic reason for building an internal enterprise user administration and provisioning system was to connect to the HR system. This product has enabled organizations to support both internal employee systems and large-scale customer facing applications for registration, user self-service, password reset, and user profile management. The object model is designed to support the organization to customize identity information of users, groups, devices, and things. This solution can be configured to create a virtual identity with links to external systems or to create a meta-directory that centrally stores a copy of identity attributes.

2. *Key Features of ForgeRock IDM*

- Password Cycle: It is a service that allows organizations to synchronize passwords in real time to ensure uniformity across all applications. This feature in tandem with the user self-service feature significantly reduces helpdesk costs and improves the customer experience. This feature ensures compliance with a secure, centralized password policy that makes it easy for legitimate users to access the resources.

- Provisioning Methods: ForgeRock's Identity Management workflow and business process engine are used to create, read, update, and delete functions based on workflow-driven provisioning activities which include a user or device requesting access to an application, or an administrator handling bulk on-boarding or off-boarding. There is an embedded Activiti module in the product which can be used for modelling, testing, and deployment.

- Synchronization & Reconciliation: This model has the ability to sync and reconcile attributes like role and group data between connected systems. ForgeRock Identity Management connector framework provides a consistent coupled layer between resources and applications. These functions are important to ensure that identity information is clean, consistent, and accurate throughout the connected resources. A flexible synchronization mechanism that provides for on-demand and scheduled resource comparisons is a key process for audit and compliance reporting.

- Auditing Architecture: The Common Audit Framework provides a means to log data consistently across the ForgeRock Identity Platform, and enables you to correlate events and transactions. Audit topics, such as access and activity, can be configured independently delivering the data you want to the appropriate business services.

- Cloud Connection: The architecture of ForgeRock Identity Management enables support for both traditional on-premises applications as well as for cloud service based providers such as Workday, Google Apps, and Salesforce.com. As more and more services move to the cloud, it is important for organizations to simplify account creation, updating, deleting, and auditing without the cost and overhead of deploying multiple systems.

- Flexible Developer Access for Customization: An open and well-documented access layer provides the user interfaces and public APIs for accessing and managing the ForgeRock Identity Platform, Identity Management repository and all its function. The open framework for developers is critical as organizations change and so does their identity framework. An open framework provides developers with direct access to manage functionality.

B. *ForgeRock Access Management*

ForgeRock Access Management [6], built from the OpenAM open source project is a single, unified solution that provides the most comprehensive and flexible set of services required for consumer facing identity and access management. Most of the legacy identity vendors have traditionally delivered different products on single sign-on (SSO), social sign-on, adaptive authentication, strong and mobile authentication, federation, self-service, adaptive risk, web services security, and fine-grained authorization. All these functionalities are delivered by ForgeRock as a single, unified offering. Organizations can use the access control services they need in a centralized way

1. *ForgeRock OpenAM Architecture*

The solution has an inherently unique architecture to support use cases from complex enterprise access control, devices, or things, to multi-protocol federation, to enabling SSO for cloud systems. ForgeRock Access Management consists of a single, self-contained Java application, service components such as stateful or stateless session management, client-side APIs and REST, service provider interfaces to enable custom plugins, and policy agents for web and access policies to protect web sites and web applications.

Organizations with existing internal access management solutions can easily integrate ForgeRock Access Management into their environment through API services or through the token translation service. It has the capability of maintaining all installation and configuration capabilities within one application which simplifies deployment of new internally or externally facing services.

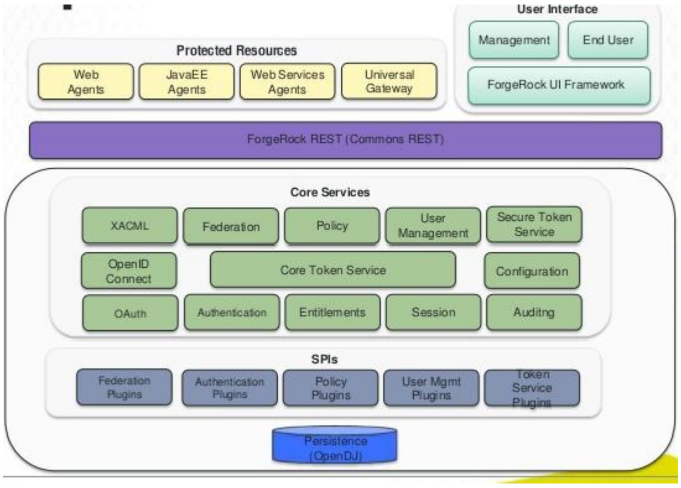

Fig 2. ForgeRock OpenAM Architecture

Agent configuration, server configuration, and other tasks are simplified so they're repeatable and scalable. This makes it easy to deploy multiple instances of the solution without additional effort. The embedded ForgeRock Directory Services eliminates the need to configure a separate directory to support the configuration and user stores. Users can utilize other directories such as Active Directory, DSEE or databases.

2. Key Features of ForgeRock IDM

- Authentication
- Adaptive Risk Authentication
- Authorization
- Federation
- Single Sign-On (SSO)
- User Self-Service and Social Sign-On
- Developer Friendliness and Open Standards
- High Availability and Scalability
- Common Auditing Architecture

IV. KEY DIFFERENTIATORS OF FORGEROCK SOLUTION

Following are the key differentiators that make an organisation select ForgeRock solution over other solution. These are the unique features of ForgeRock that differentiates it with other products.

- The most important feature of ForgeRock solution is that it is Open Source. ForgeRock is Java based solution and the code is available to the customers to perform customization according to their requirements.
- The ForgeRock solution is very easy to integrate into the organisation. It is scalable and the configuration and integration comes out in a single bundle of application which results into easy implementation.
- This solution can be integrated with cloud and has feasibility of Identity and Access control into Internet of Things.
- ForgeRock OpenIDM consists of the Connectors which acts as a bridge between various departments of organisation and the directory service for the identity provisioning. Various Connectors can be framed according to the structure of organisation to serve the purpose of Identity Management.
- There is a simple GUI as well as backend provision through code to design the roles into organisation and assigning users to the framed roles.
- The workflow of the organisation can be framed through Java Eclipse programming tool or any other source and implemented into the solution according to the requirement of the organisation regarding Identity and Access control.
- Social Login using Facebook, Password policy, SSO and Multifactor Authentication can be implemented with the help of this solution.
- Open DJ which acts as a directory services for ForgeRock solution can be customized by adding attributes according to the need of the organisation.

The availability of code and ease of implementation of ForgeRock solution act as the most distinct feature in comparison to proprietary solutions. This distinct feature gives the organisation the comfort to implement the solution as per their requirement of Identity and Access control.

V. CONCLUSION

Identity and Access Management solution have become mandatory for an organisation from the security perspective. This paper gives a brief idea of the various types of Identity and Access Management solutions available in the market. This segregation of solutions gives the organisation the space to select the solution as per their requirement in line with their budget. ForgeRock IAM solution has emerged as one of the go to solution because of its Open Source feature. The migration of resources to Cloud and Internet of Things will require accessibility of Identities and hence security will be a key aspect of these Identities and their access control. Organisations should implement an Identity and Access Management solution taking these factors into consideration.

ACKNOWLEDGMENT

I am very thankful to my guide Prof. Sangeeta Nagpure for her invaluable guidance and advice in writing this research paper. I am also thankful to Prof. Shailaja Gogate for giving me this opportunity to work in Tech Mahindra as an Intern in Identity and Access Management domain of E-Security. This internship gave me a platform to do research in Identity and Access Management.

REFERENCES

[1] Manav A.Thakur and Rahul Gaikwad, “User Identity and Access ManagementTrends in IT Infrastructure- An Overview,” in 2015 International Conference on Pervasive Computing (ICPC).

[2] Nitin Naik and Paul Jenkins, “A Secure Mobile Cloud Identity: Criteria for Effective Identity and Access Management Standards,” in 2016 4th IEEE International Conference on Mobile Cloud Computing, Services and Engineering.

[3] I.Indu and P.M.Rubesh Anand, “Identity and Access Management for Cloud Web Services,” in 2015 IEEE Recent Advances in Intelligent Computational Systems (RAICS), pp. 406-410, December 2015, Trivandrum, India.

[4] Matthias Hummer, Michael Kunz, Michael Netter, Ludwig Fuchs and Gunther Pernul, “Advanced Identity and Access Policy Management using Contextual Data,” in 2015 10th International Conference on Availability, Reliability and Security.

[5] Suryadipta Majumdar, Taous Madi, Yushun Wang, Yosr Jarraya,Makan Pourzand, Lingyu Wang and Mourad Debbabi, “Security Compliance Auditing of Identity and Access Management in the Cloud: Application to OpenStack,” in 2015 IEEE 7th International Conference on Cloud Computing Technology and Science.

[6] https://www.forgerock.com/platform/access-management/

[7] https://www.forgerock.com/search/white+papers+on+Identity+Management/