International Journal of Applied Research 2020; 6(5): 482-487

ISSN Print: 2394-7500
ISSN Online: 2394-5869
Impact Factor: 5.2
IJAR 2020; 6(5): 482-487
www.allresearchjournal.com
Received: 16-02-2020
Accepted: 20-04-2020

Pradeep Chintale
Lead Cloud Solution Architect,
Comcast Company,
Philadelphia, USA

Corresponding Author:
Pradeep Chintale
Lead Cloud Solution Architect,
Comcast Company,
Philadelphia, USA

Designing a secure self-onboarding system for internet customers using Google cloud SaaS framework

Pradeep Chintale

Abstract
This paper proposes a conceptual framework for the secure self-onboarding of self- internet customers through Google Cloud SaaS platform. It solves the main issues of security, usability, data privacy and sharing, and expansibility. The proposed system is developed with advanced authentication methods, clean design of the interface and strong integration possibilities. In combination with customer convenience and protection, this framework should minimise the challenges of obtaining clients' information while adhering to the legal guidelines on data protection.

Keywords: Self-onboarding, security architecture, data protection, authentication, scalability, integration, compliance, cloud-based systems

1. Introduction
The introduction included in this paper focuses on the need of the secure self on-boarding systems within the broadly defined Internet based customer acquisition environment. Due to the realisation of operating online, there has been the need to ease the onboarding process for businesses. This section starts with explaining the history of customer onboarding process and recognizing the shift from manual to the automated and self-service approach. This paper looks at how this has been a result of the following trends and factors like the element of cost cutting, efficiency in the usage of the interface or platform, and globalisation.

1.2 Problem Statement
The problem statement expands on the issues that organisations might encounter in the process of using safe SSO systems. It relates to such aspects as user convenience and strict security, stressing on the threats that may be caused by the lack of proper check and balance measures and data protection. In the introduction, it is also mentioned how compliance is… a question and how the threats are constantly changing for organisations.

1.3 Objectives
The objectives of the present research are stated below.
- To develop a framework on how the self-onboarding system formation can be made secure, the SaaS providers that need to be considered are Google Cloud.
- To analyse and adapt sound means of identification when conducting the agreement, and to exclude the threats and dangers to security, and when preparing the outcome to give comfort to the user.
- To develop recommendations for preserving data security and preserving the regulation of privacy during the onboarding process.
- To adopt more effective and enhanced patterns of monitoring and the fresh systems of reporting of incidents for safety.

2. Self-Onboarding Systems
2.1 Definition and Importance
Self-Onboarding can be regarded as one of the most innovative strategies in customer acquisition and product service start. These auto-propelled systems allow new clientele to sign up, and get an identity check, and obtain services without interacting with actual people. The relevance of such systems is in its efficiency to cut upon costs, simplify processes, and

and make the experience for the customers pleasant [1]. Many organisations are shifting to self-onboarding systems due to the growing market competition in the different sectors, including financial, e-commerce, and others.

2.2 Current Challenges in Self-Onboarding

The self-onboarding systems have their challenges in some ways. Fraud and identity theft are one of the fears because personal data is used to produce physical products with photos on them. In integrating technology into social systems, since most of them do not entail direct physical contact, the issue of confirming users' identity usually becomes difficult. Thus, it was challenging to balance the user experience on one hand, as well as having effective measures of security on the other hand. Challenges in relation to technical factors are also common in the onboarding process and they include system crashes or compatibility of systems used across various devices [2]. Moreover, actual implementation of these systems is complicated by the fact that they have to be adjusted to various regulations of different countries.

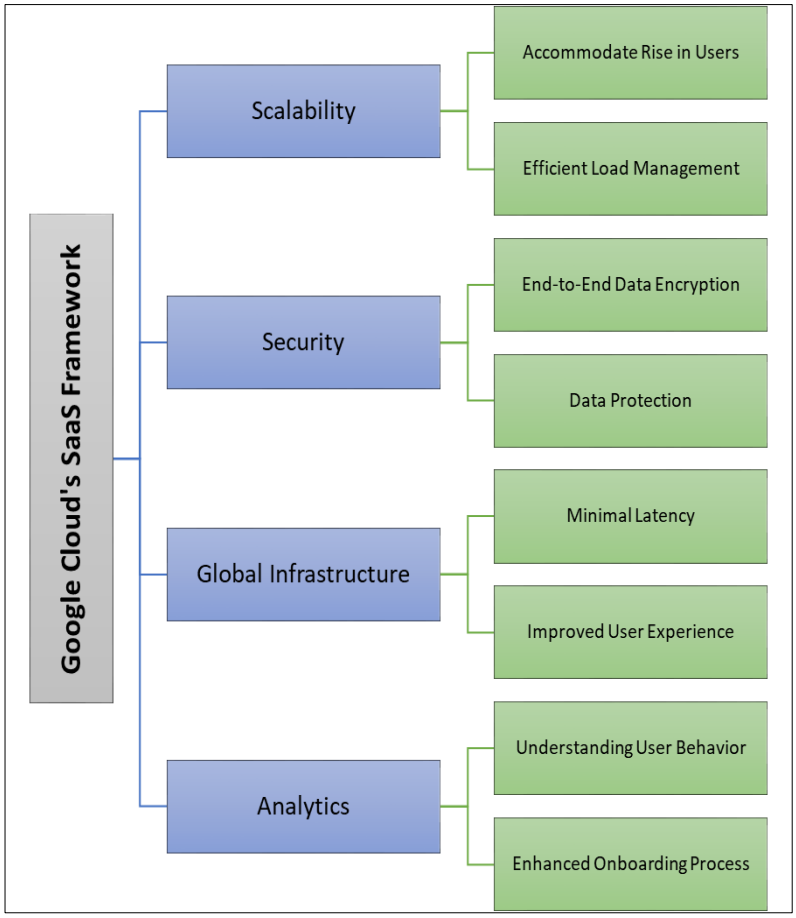
2.3 Security Considerations

An important consideration or a requirement that has to be taken care of is the security in self onboarding systems. While conducting their registrations and onboarding procedures, such platforms should pay sufficient regard to the safety of users' identification data and their money. For instance the employment of a number of factors to closely monitor the several attacks that occur in cyberspace, the encryption algorithms and the mechanisms for real time fraud detection must be core. Moreover, retaining the data, many countries have enforced certain regulations that are to be complied with, for instance, GDPR and CCPA. As for social risks, organisations must also protect themselves against these threats because hackers are always actively looking for vulnerabilities in the organisation's structures and closing them [3]. It is still very difficult today to work towards the goal to accomplish self-onboarding and, at the same time, keep the friction for the user of such systems to the absolute minimum.

3. Google Cloud SaaS Framework

3.1 Key Components

Before developing the vision of self-onboarding for a given organisation, there are best practices that need to be considered, based on the Google Cloud SaaS Framework to ensure the SaaS firm has a strong foundation. It includes a number of services and tools which are aimed to help in creation, implementation, and maintenance of software as a service application. Some of them are GKE for a performant container cluster and orchestration tool, Cloud Identity to manage access controls and authentication, and Cloud Storage to address the data organisation and protection. Also, the framework makes use of Cloud Functions for serverless computing which means that the developers can design applications that are flexible and triggered by events [4]. The said components pull together in providing a one-stop shop for SaaS solution development.



(**Source:** Self-Designed)

Fig 1: Google Cloud's SaaS Framework

3.2 Advantages for Self-Onboarding Systems

Google Cloud's SaaS Framework presents some advantages for the creation of self-onboarding systems. It means that the onboarding process can accommodate a rise in the number of users as well as accommodate a decreased load efficiently. The added security measures such as end-to-end data encryption at-rest and in-transit work to protect users' information in the onboarding process at the framework. Also, the infrastructure of this platform is international which ensures that latency from one geographic location to another is kept to the minimum, therefore improving the user experience. Because of the framework's analytics, organisations can understand the behavioural patterns of the users and onboarding process, which can be enhanced over time.

3.3 Integration Capabilities

Google Cloud SaaS Framework has a lot of integrations as one of its key advantages. It provides endless API and connectors that can easily be interfaced with other systems as well as third party services. Such flexibility allows to integrate all sorts of identity verification services, payment gateways, and customer relationship management tools into self-onboarding systems of an organisation. It is also embraced by hybrid and multi-cloud architectures, which allows easy migration from existing systems that the adopting organisations were using before adopting cloud-based self-onboarding solutions [5]. Moreover, it supports open standards; thus, interoperability and vendor lock-in issues are minor problems.

4. Security Architecture Design

4.1 Authentication Mechanisms

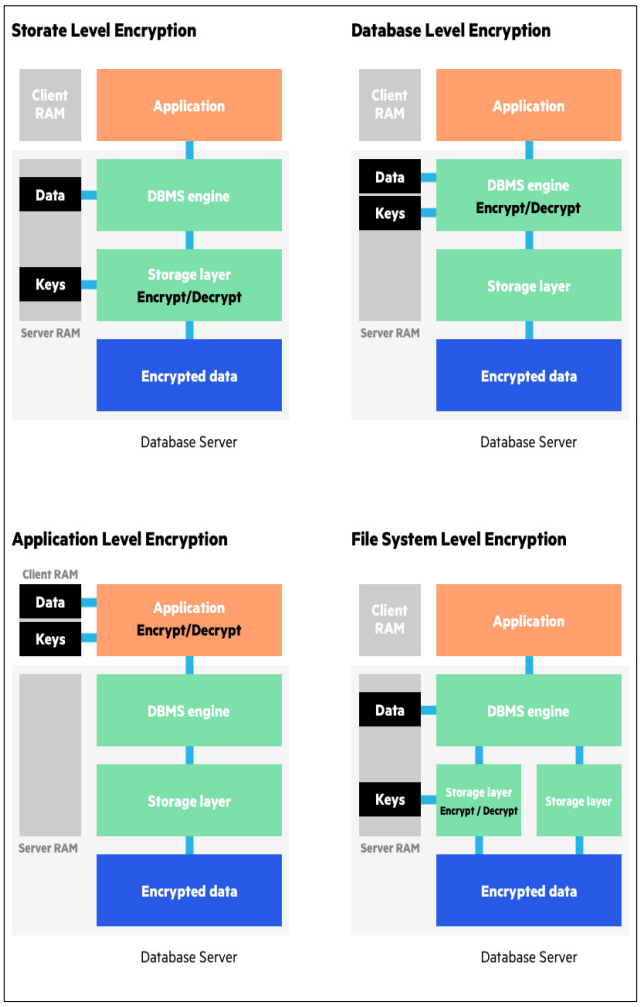
The security architecture of a self-onboarding system based on the Google Cloud SaaS Framework ensures extensive measures on the aspect of authentication. Multifactor authentication is also considered to be essential; accordingly, a user is asked several questions to confirm that he or she is the one who is trying to enter. This can be information that the user knows such as a password, an object such as a mobile device and even body attributes such as fingerprints. The system specifies Google Cloud Identity for user authentication to provide functions of SSO and compatibility with other identity solutions [6]. Also, risk-based authentication is used to adapt the security level of different users and interactions depending on location, device, and the history of users' actions.

4.2 Authorization Models

The security must be maintained from the beginning till the last step of onboarding, which calls for a fine-grained authorization model. The architecture applies the RBAC model in such a way that the users are provided with access to the resources and information that relates to the stage of onboarding. This is supported by attribute-based access control (ABAC), which takes into consideration factors and combines them to make real time authorization determination. The system also follows the principle of least privilege in which only the required access rights that are necessary for a user's job are permitted [7]. Periodic checks and revisions of the access rights prevent its corruption of the actual authorization model.

4.3 Data Encryption Strategies

When proceeding with the self-onboarding process, it is critical to safeguard personal information; therefore, the structure includes advanced data protection encryption measures. All data at rest is encrypted using Google Cloud default encryption. The data that goes through processes of transfer and storage is protected with Transport Layer Security (TLS) protocols so that the information that is shared is safe from malicious parties as it passes between the user's device and the cloud. It also applies field level encryption at the field level of a record for data elements that are highly sensitive like a social security number or a financial one [8]. This approach makes it possible to contain situations whereby unlawful intrusions happen at the database level, while major data stands encrypted and incomprehensible.



(**Source:** https://www.imperva.com)

Fig 2: Data Encryption Strategies

5. User Experience Considerations

5.1 Intuitive Interface Design

The self-onboarding system intends to uphold an easy-to-use design since user convenience is an important aspect of the system. The design is quite simple yet intuitive, and there is a logical flow from one step in the onboarding process to the next. GUI and icons provide support to users so that users of the social network do not feel lost and provide indication of progress. This design approach is commonly known as 'responsive design' owing to the fact that it adapts to the screen it is being viewed on whether it is in a portrait or landscape format [9]. It is also beneficial to engage the user with tooltips and contextual help that do not interrupt the onboarding process.

5.2 Accessibility Features

Ensuring that the system would be useful for as many people as possible, it has several aspects of accessibility. Thus it complies with Web Content Accessibility Guidelines (WCAG) 2.1 standards to guarantee the system complies with Screen Readers and other devices that extends accessibility. They also comprise the action of text enlargement or reduction, contrast modification or a keyboard-only operation. Furthermore, the source of the images has descriptions for blind people and subtitles for the videos for the deaf person during the onboarding process.

5.3 Multi-device Compatibility

Watching possible devices which can be used, the self-onboarding system is made for multi-device compatibility. Responsive is used, which means that its function is well developed on such devices as smartphones and tablets. It also uses the principles of progressive enhancement, which allows it to allow a user to view contents without much difference from the one viewed on a PC on an operating system of the user's choice on a browser of the user's choice [10]. Instances of auto-save and session persistence enable users to quit and later continue the onboarding process on a different device which is quite practical since people are shuffling between several devices today.

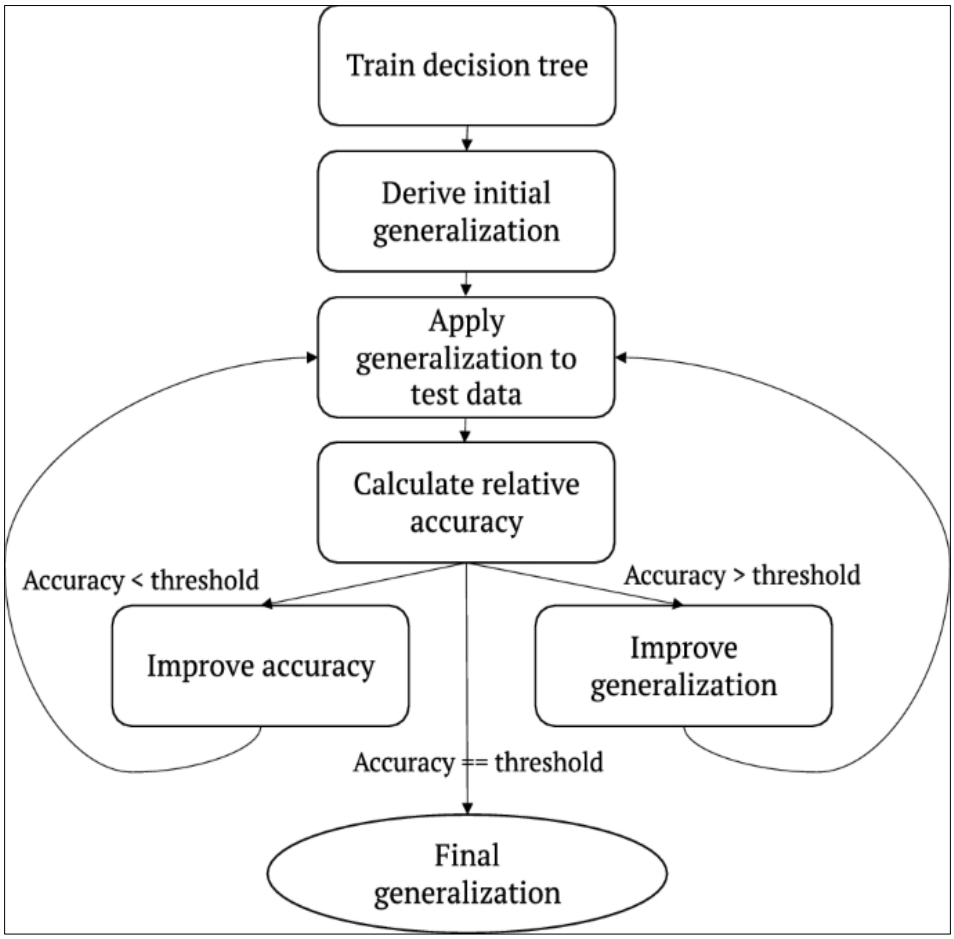
6. Data Protection and Privacy

6.1 Compliance with Regulations

The Self-Onboarding system is also created preserving the legislation of data protection laws such as GDPR and CCPA. Another strength is that it applies privacy by design since it incorporates the protection of information right from the design of the system. So, there are defaults of concurrency where users have ways through which they can opt for their data to be used [11]. The system also assists in Data subject rights including the right to (access) the own data, right to rectification and right to erasure of the data.

6.2 Data Minimization Techniques

In a bid to reduce the aspect of privacy, the system proceeds to employ the data minimization technique. At the time of on-boarding, it gets hold of only the wholesome commonly needed data, and does not apprehend lots of data. The three forms are made in an interactive way that, every time a certain information is required, the form expands to fit that information. The system also follows other retention policies that includes deletion or anonymization of data not meant to be used.



(**Source:** https://media.springernature.com)

Fig 3: Data Minimization

6.3 Secure Data Storage and Transmission

From the point of view of the means of protection demanded and defined by modern standards of security of the trading market, all the information is protected by means of the protocols for the storage and transfer of the most secure information. It also has a facility to ensure a secure connection over the network and Google Cloud storage too offers data encryption to its users [12]. Moreover, the elements of data masking and tokenization are aimed at protecting the data, which is to be classified at the levels of storage and processing.

7. Scalability and Performance Optimization

7.1 Load Balancing Strategies

The self-onboarding system has enhanced techniques of load balancing mechanisms to manage the loads of the users. It leverages the Google Cloud load balancing solutions to send the applications traffic across different regions and zones [13]. Auto-scaling is employed to fully adapt the resources that the system utilises in order to prevent it from becoming slow on periodical onboarding events.

7.2 Caching Mechanisms

The system also uses techniques like multi level caching to increase performance. That way, it incorporates the in-memory caching of the frequently accessed data in order to minimise the number of the requests to the databases and increase the speed as a result. In case of static assets, Content Delivery Networks (CDNs) are utilised to help lessen the latency for global customers by caching the content nearer to the clients.

7.3 Distributed Architecture

The architecture of the system to be developed is distributed in nature and uses microservices which are located on Google Cloud Services. This approach also permits one to scale different aspects or components of the system without directly affecting the others, and hence enhance the system's reliability. To address the issues of the initial data distribution, the database sharding techniques are applied for effective distribution of data [14]. For the execution of heavy processes, asynchronous processing is employed, and the overall workflow remains intermittent during the onboarding process for the users.

8. Monitoring and Incident Response

8.1 Real-Time Monitoring Tools

The self-onboarding system includes extensive real time checks to ensure both efficiency and safety of the system. It uses Google Cloud operational tools for perpetual monitoring of system status, user interactions, as well as the application's performance [15]. Standardised displays present general measurable results for the onboarding process and its management.

8.2 Anomaly Detection Systems

Sophisticated anomaly detection is used to detect any security threats or performance problems that may exist. It uses certain machine learning algorithms to identify the traffic's inherent patterns and highlight the spike in human activities that seem out of the norm. Thus, it is possible to prevent fraud attempts or malicious actions targeting the system from the beginning as the system detects it.

8.3 Incident Response Protocols

Pre-response plans are in place as a way of mitigating any incidents that occur in the system with considerable ease. These protocols include escalation, reporting, and response protocols. What is more, alarms are sent to the proper staff member about the crucial problems, and playbooks dictate the process to the response team [16]. Constant training both in practice and with the use of simulations is performed in order to keep these procedures effective and the institution ready for something like this to happen.

(**Source:** https://www.titanfile.com)

Fig 4: Incident Response Plans

9. Integration with Existing Systems

9.1 API Design and Management

The management of the structures is put into an efficient and well-developed API system required for integration with the previous structures. Actually, RESTful APIs follow the best practices when implemented, which makes it very user friendly and conformant [17]. For the version, documentation and management of the interface as well as for managing internal and external developers Google Cloud API management is used.

9.2 Legacy System Compatibility

Onboarding platforms employ several layers of compatibility to overcome the issue of compatibility with the existing platforms. It also recognizes these supports many data formats and protocols because it can connect to systems from the past. When needed, new approaches to supporting visualisation and other middleware applications are developed to fit today's cloud-based applications' design and structure and connect to older systems.

9.3 Third-Party Service Integration

It is easy to interact with a multitude of external services necessary for onboarding provided by third parties. The following are credit reference service, identity verification firms, credit scoring firms and CRM [18]. The precise

interoperability format and effective authentication protocols are applied to share sturdy and safeguarded data with those outside services, contributing to the enhancement of the durability of the self-onboarding system.

10. Future Enhancements and Conclusion

10.1 Potential Improvements

There is significant power and available growth in the self-onboarding system in the future. Other layers of security such as going for further biometric authentication systems such as face or voice probably can be added to it to increase security. An incorporation of chatbots powered by artificial intelligence in a platform can improve the first time user engagement especially when offering directions to the new member. Moreover, research and development in blockchain applications for Decentralised ID is another field that can possibly provide better security and user control.

10.2 Emerging Technologies in Self-Onboarding

There are possibilities with self-onboarding that can be developed by adopting new technologies like augmented reality (AR). With the aid of AR one could have a means of identifying different procedures and the difficult steps that define them. The recommendations could also be made though AI algorithms which would suggest the subsequent actions based on the onboarding user behaviour.

10.3 Summary of Key Findings

It can be concluded that this paper has made a clear explanation on the strategy that needs to be followed for the implementation of a self-onboarding system within the confines of security and using the Google Cloud SaaS Framework. In general, it has offered answers to some of the most basic questions that concern its security, the system's human interaction interface or GUI, the manner by which data is managed or processed, modularity for distinct job implementations, and compatibility with other systems. With the proposed system, it is possible to improve the organisational-instrumental support for the simultaneous acceleration and enhancement of the customer's onboarding; to establish the prerequisites for the further innovative development of digital customer acquisition.

Reference

1. Dapp MM, Klauser S, Ballandies M. Finance 4.0 design: technical report. ETH Zurich. 2019.
2. Autio T. Developing central documentation in an equipment delivery process in a global technology organization. [unpublished report], 2017.
3. Bank D. Interim report as of June 30, 2018. Frankfurt am Main, 2018.
4. Tsai WT, Huang Y, Shao Q. EasySaaS: a SaaS development framework. In: Proceedings of the 2011 IEEE International Conference on Service-Oriented Computing and Applications (SOCA); 2011, 1–4. IEEE.
5. Padhy RP, Patra MR, Satapathy SC. X-as-a-service: cloud computing with Google App Engine, Amazon Web Services, Microsoft Azure, and Force.com. International Journal of Computer Science and Telecommunications. 2011;2(9):1–6.
6. Li D, Peng W, Deng W, Gai F. A blockchain-based authentication and security mechanism for IoT. In: Proceedings of the 2018 27th International Conference on Computer Communication and Networks (ICCCN); 2018, 1–6. IEEE.
7. Foster I, Kesselman C, Tsudik G, Tuecke S. A security architecture for computational grids. In: Proceedings of the 5th ACM Conference on Computer and Communications Security; 1998, 83–92. ACM.
8. Gai K, Qiu M, Zhao H, Xiong J. Privacy-aware adaptive data encryption strategy of big data in cloud computing. In: Proceedings of the 2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud); 2016, 273–8. IEEE.
9. Stone D, Jarrett C, Woodroffe M, Minocha S. User interface design and evaluation. Elsevier, 2005.
10. Dong T, Churchill EF, Nichols J. Understanding the challenges of designing and developing multi-device experiences. In: Proceedings of the 2016 ACM Conference on Designing Interactive Systems (DIS); 2016, 62–72. ACM.
11. Park G. The changing wind of data privacy law: a comparative study of the European Union's General Data Protection Regulation and the 2018 California Consumer Privacy Act. UC Irvine Law Review. 2019;10:1455–84.
12. Chen D, Zhao H. Data security and privacy protection issues in cloud computing. In: Proceedings of the 2012 International Conference on Computer Science and Electronics Engineering; 2012;1:647–51. IEEE.
13. Wang K, Zhou X, Li T, Zhao D, Lang M, Raicu I. Optimizing load balancing and data-locality with data-aware scheduling. In: Proceedings of the 2014 IEEE International Conference on Big Data (Big Data); 2014, 119–28. IEEE.
14. Geimer M, Wolf F, Wylie BJ, Ábrahám E, Becker D, Mohr B. The Scalasca performance toolset architecture. Concurrency and Computation: Practice and Experience. 2010;22(6):702–19.
15. Kiani A, Salman A, Riaz Z. Real-time environmental monitoring, visualization, and notification system for construction H&S management. Journal of Information Technology in Construction. 2014;19:72–91.
16. Porras PA, Neumann PG. EMERALD: event monitoring enabling response to anomalous live disturbances. In: Proceedings of the 20th National Information Systems Security Conference; 1997;3:353–65.
17. Pärn EA, Edwards DJ. Conceptualising the FinDD API plug-in: a study of BIM-FM integration. Automation in Construction. 2017;80:11–21.
18. Ecer F. Third-party logistics (3PLs) provider selection via fuzzy AHP and EDAS integrated model. Technological and Economic Development of Economy. 2018;24(2):615–34.