International Journal of
**Technology and Systems**
*(IJTS)*

# REVIEW OF DIGITAL IDENTITY MANAGEMENT SYSTEM MODELS

Zabron Githongo Mburu, Dr. Lawrence Nderu and Dr. Mwalili Tobias

IPRJB
INTERNATIONAL PEER REVIEWED
JOURNAL AND BOOK PUBLISHING

# REVIEW OF DIGITAL IDENTITY MANAGEMENT SYSTEM MODELS

[1*]Zabron Githongo Mburu
[1]Post Graduate Student: Jomo Kenyatta University of Agriculture and Technology
School of Computing and Information Technology
*Corresponding Author email: zgmburu@gmail.com

[2*]Dr. Lawrence Nderu
[2]Lecturer: Jomo Kenyatta University of Agriculture and Technology
School of Computing and Information Technology
Email: lnderu@jkuat.ac.ke

[3*]Dr. Mwalili Tobias
[3]Lecturer: Jomo Kenyatta University of Agriculture and Technology
School of Computing and Information Technology
Email: tmwalili@jkuat.ac.ke

## Abstract

***Purpose:*** Public and private Institutions are presently facing challenges in the control of users accessing information via online platforms. Institutions presently control classified user identity information via online platforms. Trends indicate there is insignificant control of classified information within organizations, making it one of the serious threats facing governments and organizations. Digital Identity Management Systems (DIMS) are very vital in organization infrastructure for the purpose of authenticating users and supporting unlimited access control of services. The core intention of this paper is to review the existing digital identity management models and analyze the extent of the research work.

***Methodology:*** The paper will review the characteristics of Digital Identity Management Models and evaluate on how trust and privacy issues impact or influence the establishment of an effective digital identity management system.

***Findings:*** This paper reviews existing digital identity management system models. Regulation of information in cases when the entities requiring access to it are both highly diverse and spread is among the most significant challenges to effective identity management. A variety of normal technical questions also faces the field, for example, the manner in which information in centralized and distributed databases can be controlled. In a bid to ensure that information related to authorization and authentication is up to date and dependable within an organization’s systems of information, handling personnel has been a major concern of identity management systems.

***Unique contribution to theory, practice and policy:*** A hybrid digital Identity Management System model approach that will aim at solving the gaps identified in the existing digital identity models will be the future paper’s subject of concern.

**Keywords:** *Digital Identity, Silo System, Federated IDMS, Centralized IDMs, User-centric identity systems.*

## 1.0 INTRODUCTION

States and government bodies have an obligation to convey identity and keep citizen's records. The role of the government is not only to guarantee nationals' rights and security, but also to collect vital information for both public and private use. Users would now be able to perform web-Services with their characters secured utilizing Digital Identity Management Systems (DIMS). Digital identities represent a system or group of systems which allows the formal recognition of the entity inside a scenery towards what is important. Digital identities are the advanced description of the data thought about a particular individual or association. An entity can be characterized as a description of a man or element in a particular space. An entity typically denotes to a specific entity. An entity may include a few personalities inside a given space. For instance, an entity might be both a worker in an organization and a client in the same organization.

Globalization, data, and correspondence transformation are the primary explanations behind governments to change the method for utilizing data and conveying open merchandise and ventures to populations by organizing service delivery.  This requires the capacity of sharing very large information and data over an extensive variety of inward and outside processing frameworks and handling its usage. The wide access of shared information relies upon electronic devices.

Identity is a word that depicts "the reality of being whom or what a person or thing is" (O. Dictionaries," oxforddictionaries.com," 2015.) To English dialect, the word identity was gotten from Latin word idem, which means same in English. Identity conveys in itself the significance of similarity, having indistinguishable qualities from another identity. Further, as the definition says, identity can also refer to identity of things as opposed to simply persons. According to Jain, 2016, e-government systems support public service delivery through web-based applications. The process of e-governance relies on data mining, which avails important information required for service delivery to the citizens.

Electronic government is a phrase used to describe the manner in which Information Technology (IT) and other technologies like online media platforms are used with the aim to improve service delivery in public administration. E-governance broadens and improves partnership between governments and other sectors, which streamlines public administration (Alenezi et al., 2015). As E-Government fundamentally depends on the Identity Management (IDM) utilized in the E-Government framework essentially dictates individual data from administration offices, natives and organizations will have. Electronic Identity Management (eIDM) alludes to the administration of advanced personalities or computerized character information by amplifying security (data assurance) and limiting expense and repetitive exertion. The execution and utilization of dependable arrangement of eIDM assists nationals, organizations, and parastatals to easily recognize themselves and ensure their exchanges precisely and rapidly. Technology divides information into set of qualities that can be overseen by specialized means, referred as digital entities. Contingent upon the circumstance and the setting just separation of these ascribes are expected to depict to an individual in the world, both digitally and physically, supposed partial characters. An IDM avails the platform in which the portion identities are controlled in the digital world.

Identity depicts an arrangement of one of a kind qualities or attributes that differentiates those of one individual to another. Commonly those attributes are derived from the demographic characteristics of an individual such as the place of birth and physical appearance and an assortment of social variables including place of residence, occupation et cetera. In most countries people are issued with identities at birth which keep on being utilized for the duration of their lives.

An identity comprises of an arrangement of qualities and attributes, known as identifiers when utilized for identification. These attributes may have different properties, for example, transiency or lasting, self-chose or provided by an expert, reasonably for user understanding or by personal computers. The advantages of receiving eIDM involves putting away data in digital where it can be effortlessly gotten to and exchanged at whatever point required, guaranteeing a safe, advantageous and compelling method for recognizing both an individual and service provider, and defending and ensuring access to access data. Moreover, it enhances the nature of administrations to be conveyed, limits administration cost, and builds trust in dependable distinguishing proof and approval of clients, which thus empowers secure and powerful everyday data exchanges between public offices. Hence, by accepting efficient identity management in e-governance; governments can enhance service delivery and attain operational excellence in the delivery of government services that leads to customer satisfaction.

According to Bertino (2012), identity is a chain of events that takes place from the enrollment process to the validation of credentials and management of data around an element that is adequate to distinguish that element in a specific setting. Digital identity therefore eliminates the need for a person to be available when making interactions and transactions. Rahaman and Sasse (2011) describes this feature as the identification processes’ disembodiment.

## Digital Identity Management System Validation

Numerous requirements have been developed for validation purposes before gaining entry to online services. There are distinct levels of identity management systems that differ according to different designs, implementation, and functionality. These include the federated Silo, Centralized, and user-centric systems. Federation identity management is characterized as an affiliation involving different groups of service providers and identity providers. The way the different service providers have shaped a relationship between themselves implies that they have mutual trust between themselves and communicate between themselves. The federated identity management (FIM) is often involved at the point when these messages contain the verification and approval certifications of clients, and thus, enabling customers from one arrangement to get to supplies in a federated structure.

In order to access other sites within the federation, users can utilize credentials offered by a single or multiple identify providers. FIM gives users an opportunity to validate and apply identity information from data dispersed across different domains. The data sharing across domains breaches security system in place and possibly causes infringes privacy rights. A validation process must contemplate how the identifiers and credentials should be acquired. In the event that the ease of use is poor, at that point the authentication itself will be feeble in light of the fact that clients cannot deal with their credentials sufficiently. In such manner, it is fascinating to see that SPs generally have automated systems to oversee identity and authentication, though clients typically oversee credentials manually. From a client point of view, an expanding number of identifiers and credentials quickly turn out to be absolutely uncontrollable.

## Identity Federation

Identity federation refers to a plan that connects accounts of clients kept up unmistakably by various partnerships. The idea of system identity is a catalyst for mechanization of Web Services in computing for clients for their sake while securing protection of identifiable data. A single authority or detached entity is able to, through a relatively simple identity management model, play the role of an absolute provider of credentials and user identifier for service providers.

In a typical user identity framework, an individual is able to use services offered by all providers while applying a similar credential or identifier. For instance, this is achievable through acquisition of a PKI in which certificates to all users of the domain are provided by a specific Certificate Authority (CA), or subsidiary, or cross-certified Certificate Authorities thereof. A good example of identifier name space is email addresses. They are that globally unique. As such, users only require a specific group of credential and identifier to be validated by every SP's, as long as protocols of operating a PKI have been met.

On the international platform, it could be disastrous to have the unique identifiers in some forms such as email addresses. They are acquired discretely; users have the freedom to ma-nipulate email addresses, besides a single person can operate multiple email addresses simultaneously. This is impractical when it comes to using other computer applications, which are only installed using the unique identifiers once.

## Related Work

This part provides a brief analysis of hypothesis and frame works created and applied in evaluating, addressing and knowing people and hierarchical appreciation and use of new technologies. These frameworks have been developed after extensive research but were not embraced because of the slow approval and defense. A number of digital identities have been put into operation using distinct technical and architectural model.

Digital Identity: Online platforms give users an opportunity to interact with the technology. During the interaction users, leave footprints that are gathered by computer programs known as cookie. This information is then used to give a projection about the taste and preferences of the user. These impressions provide tracks from electronic mails, going to sites, buying things on the web, postings and opinions made on social media platforms such as Facebook, texts, and personal profile in different databases. Such a wonder suggests, to the point that, an entity can have various attributes relying upon the specific situation, which on a very basic level reclassify the notion of identity.

With technological advancements, digital identity will pro-vide individuals an opportunity to access services. For in-stance, accessing financial services could be improved through the use of digital identities by getting rid of the paper work and having a digital way of verifying identities of customers. Digital identity along these lines expels the necessity for parties to be available amid exchanges and associations. According to Rahaman and Sasse, (2011) digital identity is the disembodiment of the process of identification. Digital identity, guarantees an absence of restriction to a specific area or system and hence guaranteeing more extensive, dispersion of personal information. It is thus vital that such factors are additionally tended to in identity to provide resultant digital identity. Figure 1 illustrates a set of attributes that once aggregated form the digital identity management system.

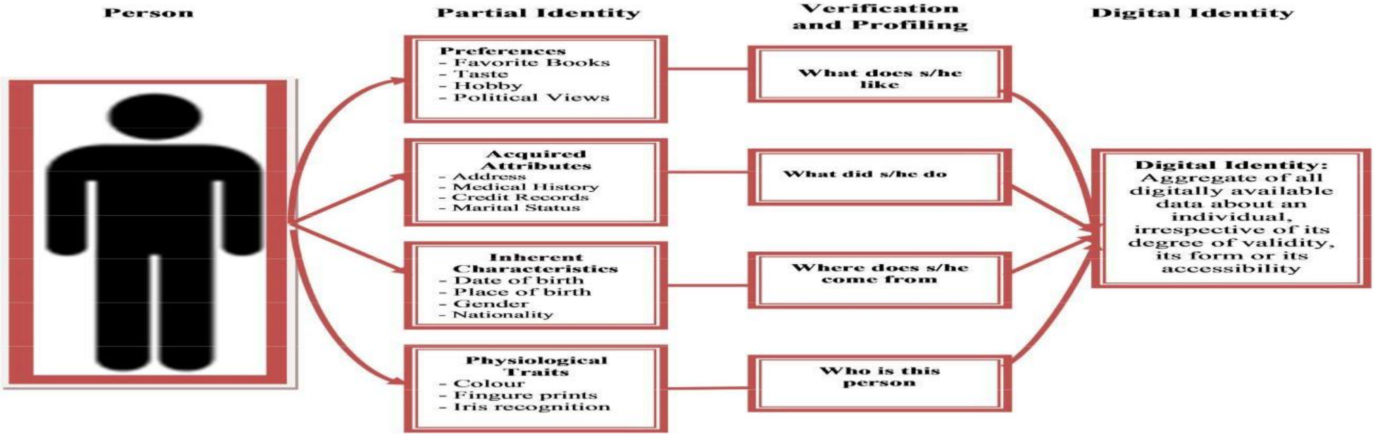

**Fig. 1. Digital Identity Source: Adjei, J. K. (2013). A Case for Imple-mentation of Citizen Centric National Identity Management Systems**

Silo Identity Systems: With a primary goal of satisfying its essential goals, an organization generally plans and works out its framework of Silo Identity Management System without external interference. A good example is the active directory. Such a DIMS, for the most part does not permit associations with different DIMS and hence the identity provider likewise plays the part of service provider (SP), to an extent that it deals with the authentication tokens and name space for every one of those who use it. The Service Provider likewise confirms users in light of their identifier-token pairs amid benefit get to. Technology users may be permitted, provided they are remarkable inside the name-space, to characterize their own identifiers.

Characteristics of Silo Identity Management Model The silo Identity Model have the advantage of having unlinked capacity. Because the system is not linked to some system, users' characteristics in a single system cannot be effectively connected to various identifiers of similar users in different domains. Furthermore, a security breach on one of the silos does not expose the vulnerability different systems. However, Silo Systems are extremely inflexible in that they do not bear the cost of users the comfort of likability where vital, bringing about the utilization of a variety of credentials and identifiers relying upon the unique situation.

Existences of multiple user credentials, identifiers, accounts and are generally extremely hard to oversee and in this way user, regardless of how vulnerable the systems are, shift their attention to different silos and use similar identifier. In addition, because of effort duplication, the Silo Model misuses resources. For example, personal data is stored in each of the identity silos in spite of the fact that this could avoided if the information is to be public. Figure 2 shows the Silo Digital Identity Model where each service provider stores personal information of the data subject.

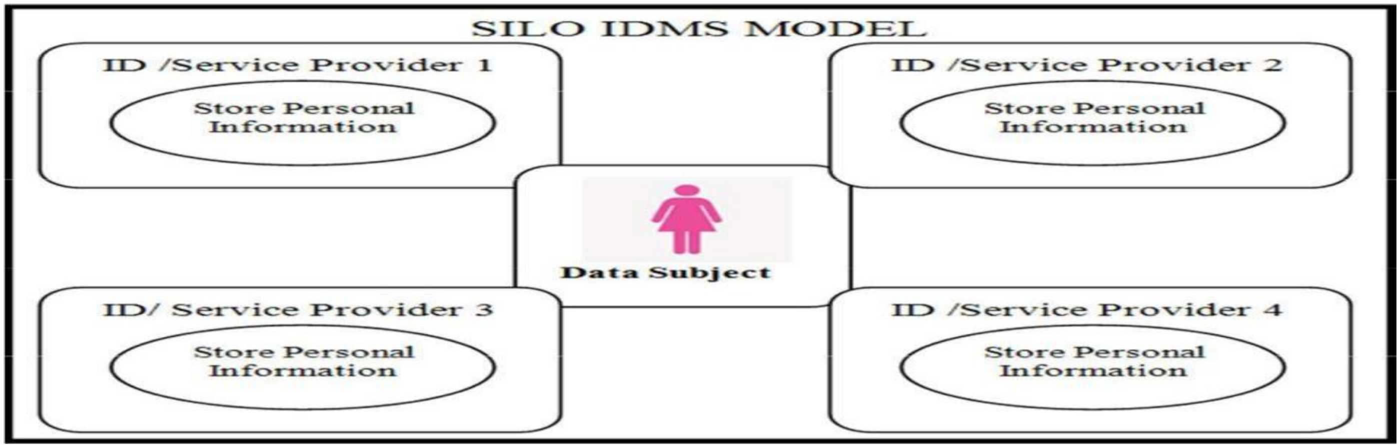

**Fig. 2. Silo Identity Systems Source: Adjei, J. K. (2013). A Case for Implementation of Citizen Centric National Identity Management Systems**

In addition to the idea that it exposes personal information only to the SP, the simplicity of its deployment for the SPs is one of the advantages of this model. However, since it leads to password fatigue and identity overload for those who use it to obtain services from multiple and different SPs. The principle of security usability is violated in this case. Further, for infrequently used SPs, users tend to forget passwords. A significant barrier to usage arises from both the fear of forgetting or forgotten passwords, which consequently, makes the SPs not to operate to their full capabilities. For services that are significantly sensitive, especially where a highly secured recovery of password is required, the cost of providing services tends to increase due to the forgotten passwords.

Centralized Identity Systems: DIMS model is one of the models that overcomes the weaknesses of the silo model by assembling the autonomous databases into a single model. In this manner in the centralized model, user information is stored in autonomous sections of the different application silos, and information is relayed to centrally databases of service providers. Because of the centralized idea of the model, every user is capable of utilizing similar credentials and identifiers to get to various services, while every one of the SP validate the user through a similar credentials before giving access to their service.

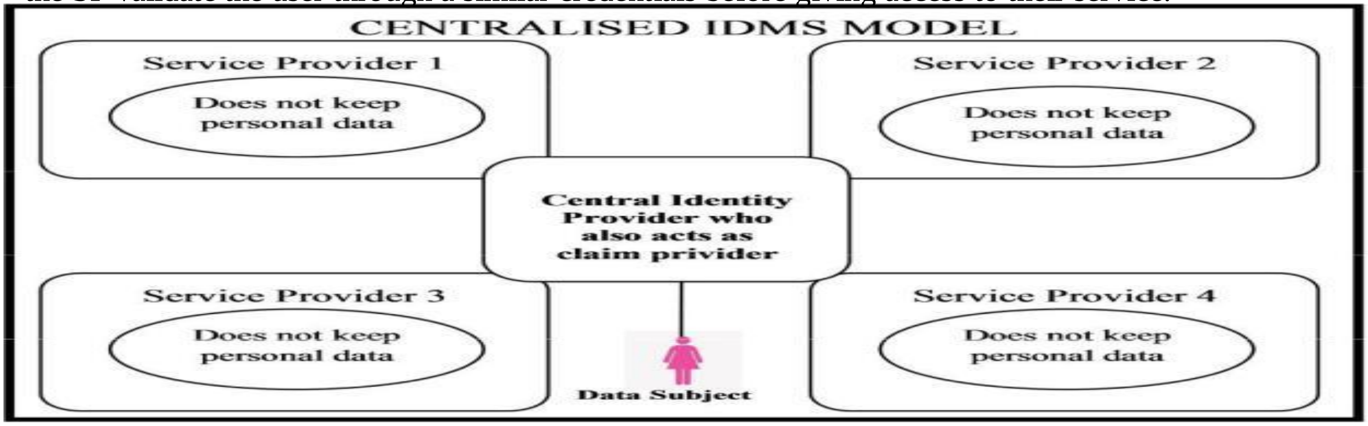
CENTRALISED IDMS MODEL
Service Provider 1
Does not keep personal data
Service Provider 2
Does not keep personal data
Central Identity Provider who also acts as claim privider
Service Provider 3
Does not keep personal data
Service Provider 4
Does not keep personal data
Data Subject

**Fig. 3. Centralized Identity Management Systems Source: Adjei, J. K. (2013). A Case for Implementation of Citizen Centric National Identity Management Systems**

### Characteristics Centralized DIMS Model

The ability of the model to offer good usability through SSO is one of the major advantages of the model. Further, the suitability of the model is based on closed networks where the same organization such as large companies, governments, or universities manages multiple SPs. The assumption, with closed networks, is that the same authority and under one policy governs the IdP and SPs. Some of the perfect examples regarding the manner in which SSO can be efficiently implemented with an organization's corporate networks include authentication networks based on Active Directory and Kerberos.

Nonetheless, the issue that the model has no suitability for execution in open environments in which a common authority or policy governs SPs is its major disadvantage. Actually, the ideology that a single IdP is acceptable by SPs to carry out authentications and manage identities in their behalf is not a possibility. Technically, the principle of user-centric privacy protection of minimizing cases where personal information is exposed would be violated. Ideally, the personal information should not be accessible through the centralized IdP.

Federated Identity Management (FIM) Systems: The FIM model is among the most comprehensively and extensively developed models among the preceding ones. In a bid to ensure digital identity information is shared safely, firms/corporations create teams with developed trust relations among themselves and referred to as Federated Identity. Technically a federated model comprises of protocols and software elements in which individual identities are managed. According to Bertino (2010), the Service Oriented Architectures can be utilized to perform the execution of IdP, SP and User, which are the core entities of a federation model.

Technically, varying organizations create trust circles or federations in a federated identity management system. When the need to deal with user identity arises, there exist service providers and identity providers who confide in each other inside these circles of trust. After which a user is capable of using the services provided by the SP, he/she could use any service provider within that federation to sign in without any need to log in a second time. While the Open Group describes it as "a mechanism in which a user is permitted to access all systems and computers through a single action of user authentication and authorization where such a user is capable of accessing permission, but the requirement to enter multiple passwords does not exist. Further, as major issues of failure of systems, human errors are reduced through single sign-on (SSO), and thus, it becomes difficult to implement but highly desirable," this is a good example of a Single Sign-on (SSO). Figure 4 below illustrates how in Federated DIMS service providers keep partial information of the user.

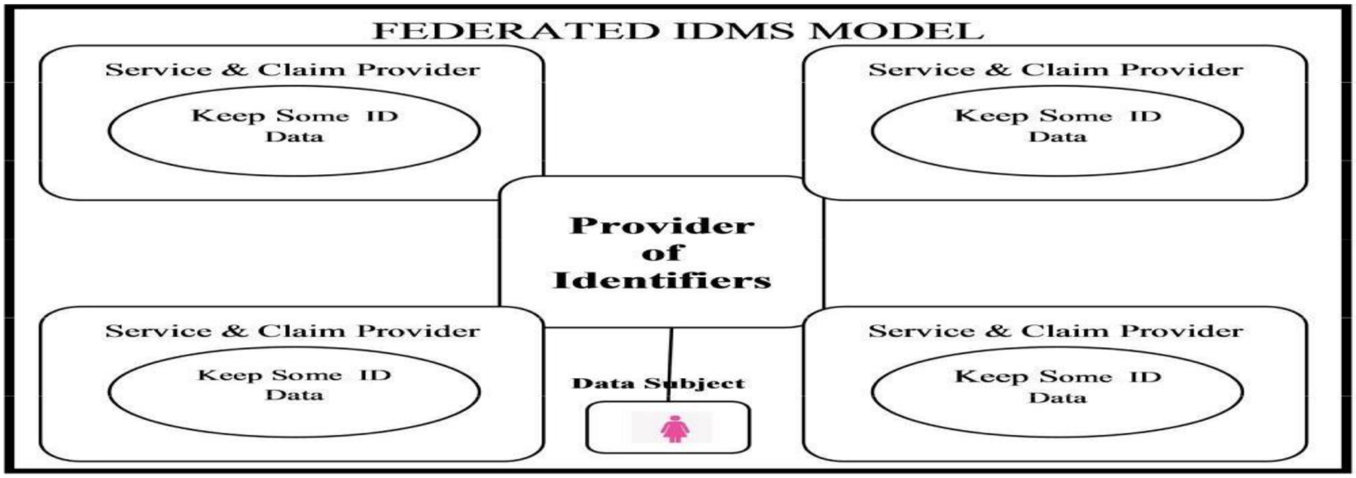

**Fig. 4. Federated Identity Management Model Source:Adjei, J. K. (2013). A Case for Implementation of Citizen Centric National Identity Management Systems**

### Characteristics of Federated DIMS Model

The ability of the model to offer SSO in open surroundings is the primary advantage of the federated identity model.

While it can, therefore, be retrofitted to the traditional silo model, the federated model is compatible. Thus, authentication systems and name spaces can keep on existing within SPs. Nonetheless, the fact that it forms technical and legal complexities is the central disadvantage of the model. In technical terms, SPs are not capable of differentiating between a security request depicting another service provider disguising as a user or reflecting a genuine request by a user of services. It, therefore, implies that SPs have to trust each other's security assertions. Further, although it could pose as a security threat, SPs are, through mapping across identifiers, capable of correlating data regarding the same user. With respect to this issue, users have to confide in SPs to safeguard their privacy.

It is possible for a federated model to be a disadvantage or advantage based on the privacy perspective. Due the mapping across identifiers, varying SPs within the same circle of trust is capable of matching personal data of the same user. In addition, while it can pose a threat, the adherence to the policy and privacy policy itself acts as the basis for protection of privacy. Where else, while only the "home" SP needs to perceive the actual identity of a user, the identity of a user within a particular silo domain of an SP can operate anonymously. However, additional protection of privacy can be provided through this aspect. Similarly, the scalability problem for the users can be solved through federated identity domains in order to have several centralized identity domains as explained in Sec. 4.4. As such, it is most likely that a user would access SPs from varying domains by making an assumption regarding the existence of multiple federated identity domains. Thus, authentication would have to be accomplished based on each domain.

User-centric identity systems: In this model, the objective is to use an approach that will give users the freedom to control their identities. Furthermore, it envisages a scenario where users can pick their desired identity provider and has the privilege to install software of their choice on their devices e.g. computer, and Smart-phone. The primary strength of the user centric model is that the determination of the credentials and characteristics of users are shared through online platforms. User privacy has been ignored in the model. With the ability to integrate a trust model, smart card solutions can be provided through a user centric model. Consequently, after a validation process, identity provider characteristics are retrievable through this model and sent to the SP (L'Amrani et al., 2016).

User-centric identity system refers to an endeavor that gives users full control in managing data flow (Cavoukian, 2012). Hence, User-centric DIMS seeks to provide flexibility in identifying and picking independent of SPs. In addition, it is unnecessary for users to reveal personal information to potential SPs to get access to service and use other resources.

In this model, the Identity providers play a trusted third-party role where they manage user account, profile data, validate users and SPs acknowledge claims or declarations regarding users from the identity providers.

Enabling the creation of providers of identity who run in the interest of users is the most essential goal of a user-centric DIMS system. Ideally, three components incorporated as part of the User-centric DIMS systems include:

1. Identity Providers - to authenticate users and act as storage for profile information and accounts of users
2. Relying Parties – facilitate the acceptance of 'claims' from providers of identity regarding users to service providers. This means having, with the user, an authen-tication dialog.
3. Identity Selectors – through this component, users have the capability to select the kind of data they can share or disclose with a particular service provider, as well as the identity provider to use. Experts believe that the complex measures of identity disclosure existing in the world physically can be emulated through the user-centric IDM.

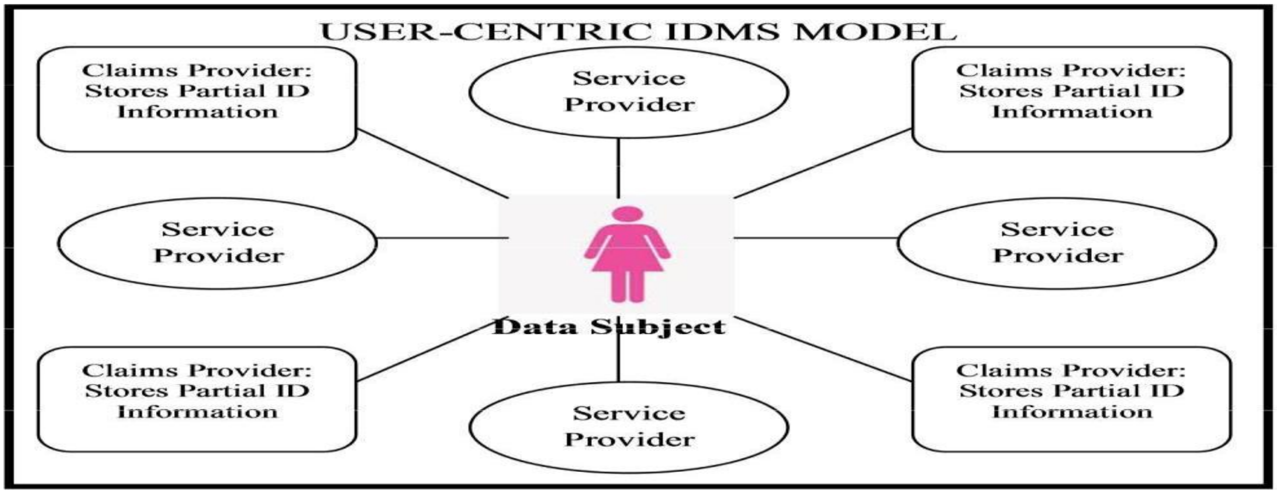
USER-CENTRIC IDMS MODEL
Claims Provider: Stores Partial ID Information
Service Provider
Claims Provider: Stores Partial ID Information
Service Provider
Service Provider
Data Subject
Claims Provider: Stores Partial ID Information
Service Provider
Claims Provider: Stores Partial ID Information

**Fig. 5. User-centric identity systems Source:Adjei, J. K. (2013). A Case for Implementation of Citizen Centric National Identity Management Systems**

Privacy-Enhancing Technologies: The issue of doubt between the depending party and user is tended to, in light of the fact that the identity provider goes about as a trusted outsider agent in a User-Centric DIMS. People can have a few distinctive identity providers, and as far as that is concerned, their data may kept in a single location. IDEMIX (IBM, 2010) and U-Prove (Microsoft, 2011) are a portion of the significant

User-Centric and security improving DIMS advancements and structures that look to help executing and interfacing gatherings to oversee claims and qualities so the depending parties that guarantee that the data is right before drawing in with the user, despite the fact that the user identity would not be disclosed. These methodologies guarantee least revelation of individual data and fine-grained delegation of approval between service providers.

According to Microsoft, 2011, U-Prove – Developed in view of a progressed cryptographic innovation and ideas, U-Prove is an endeavor to challenge the well-established problem between the privacy and assurance of identity. The situation is tended to by empowering insignificant exposure of information identity in electronic exchanges and correspondences. U-prove is an innovation that Microsoft and engineers could accept to aid in the advancement of a non-closed character and obtain display for people, organizations, and offices of governments. Along these lines, the idea of U-prove is established in the standards recommended in the metasystem of personality.

## IDENTITY MANAGEMENT SYSTEMS

To manage user privileges and roles to access resources across non-homogenous technology environments, ensure that compliance requirements are met, and establish individual user’s digital identity is the role of identity management. In their work, Thakur and Gaikwad (2015) provide a closure of IDM functionalities categorization and IDM. Similarly, as a taxonomy addressing other IDM products’ quality aspects and functional requirements, a compilation of an articulately detailed class of needs of IDM is provided in the works of Ferdous and Poet (2012). Identity management is tied in with building up identities maintained digitally for every single user, overseeing individual parts, and benefits to get to resources crosswise over non-homogenous technology conditions, and guaranteeing that consistence necessities are fulfilled.

In other works, Thakur and Gaikwad (2015) provide an outline of IDM and IDM functionalities arrangements. Fer-dous and Poet, 2012 aggregate an exceptionally set of IDM necessities as a scientific classification that tends to utilitarian prerequisites and other quality parts of the IDM items. The web page that give an IS has its personalized particular validation techniques keeping in mind the end goal to give the benefit solely to approved users. Identification methods right now being utilized on the Internet could be explained in the following manner:

a. ID/PW based verification: requiring that a unique ID be issued to the client during subscription and through a different strategy, this is the broadest authentication technique;

b. Authentication utilizing the national identity and real name of a user;

c. Authentication utilizing effectively enlisted email data; Authentication utilizing an i-PIN.

d. Authentication utilizing a public certificate: This tech-nique is normally utilized when for e banking or similar needs require fault-prove-authentication. Here, a tech-nique indicated by the public certificate issuance orga-nization is utilized to verify users.

e. Authentication through a Mobile Device: This technique utilizes the record information (client information at the season of membership, cell phone number, and so forth.) of the versatile media transmission bearer and the mobile handset’s special number (S/N).

f. Authentication utilizing biometrics: This strategy includes the check of the iris or unique mark of a user.

g. Composite authentication: This technique joins at least one of the strategies said above. The Internet condition involves a specific level of vulnerability as far as the capacity, administration, and upkeep of the user's authen-tication information relying upon the different methods and systems of authentication.

The current strategies for hacking endeavor that susceptibility has turned into a social issue. Accordingly, the proposed countermeasure against such issues is the technology of identification.The objective of a DIMS system is to ensure steady business operation rules; lessening expenses through re-engineering of business processes; improving safety and; narrowing of control over user-to applications; better performance.

1. Enrollment/Registration: Clients must experience be-ginning enlistment/enrollment forms where their historical impression, biometric impression or a blend of both are caught into the framework. The result of the enrollment procedure is the issue of qualifications or identifiers to those enlisted. In actuality, enrollment is the procedure by which a user is given exclusive rights to enter the system. The personality ap-proach, the subsequent frameworks, and the inevitable issue of certifications and identifiers are addressed during the process. The introduction of a kid or the landing of remote national who meet standards will generally stimulate the enrollment procedure in a DIMS in a nation.
2. Authorization: Upon enlistment, consent, and benefits to get to the services and resources are allocated to a person in light of n established identification policy. 3) Authentication:
   - This is the way toward setting up with a specific level of trust in the client's personality or a procedure that outcome in a man being acknowledged as approved to participate in or play out some action (E. A. Whitley, 2013).
3. Authentication: In this manner, confirmation is the way toward checking that a client is not a fraud. By either viewing of biometric information, learning of certain data, or signing into a system with a given credential, a person makes verifiable identity to access services and resources. There are numerous confirmation techniques with various degrees of affirmations, likewise alluded to as factors of authenticating, for example, things known to clients or possessed by client, as well as thing the client is such as passwords or Smart Card and passport or Biometrics, respectively.
4. Access Control: Authentication procedures bring about the process of control of access in which the system does a confirmation to verify whether a person is authorized to access the system;

5. Revocation: This regards a case when related rights being revoked and a revocation procedure is activated bringing about the credentials including when a man is no more connected with the system or on the expiry of people's rights. Such conditions incorporate when an individual finishes school, goes abroad for more than a predefined period, or the demise of a citizen.

Figure 6 shows a summary and process of identity formation.

a. Intrusion: The existing systems endanger sensitive informa-tion leading to identity fraud and leaking of information.

b. Intrasitivity: This is lack of association between the identity of a user at one area and their identity in another area, e.g. using several computer devices to access information by the same user. This leads to repetition and dissatisfaction.

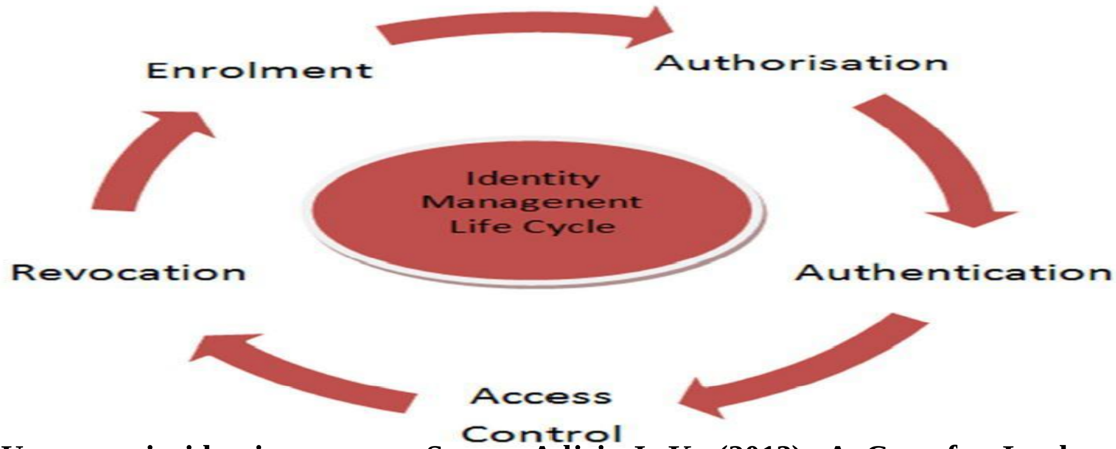

**Fig. 6. User-centric identity systems Source:Adjei, J. K. (2013). A Case for Implementation of Citizen Centric National Identity Management Systems**

### Gaps in existing Digital Identity Management Systems

Intrusion: The present personality framework is set up to take into consideration immense engendering of sensitive information. In the best case this essentially prompts the uneasiness of not knowing who has what data. In the most pessimistic scenario, genuine data spills happen which can thus prompt wrongdoings, for example, identity fraud. Along these lines, on the grounds that the system allows such simple proliferation, it is additionally extremely inclined to leaking.

Intransitivity: This is the lack of association between the identity of a user at area A and their identity at area B, where areas can be sites, or online computer games, and so forth. For the most part, in the wake of experiencing the majority of the bother of making a record or personality at one area, it is totally futile wherever else. We can henceforth call these identity intransitives. They do not exchange crosswise over domains, recreations, or destinations, aside from those inside a similar association. Hence, whatever attributes a user information sources or gathers in a single place are not important in another place. This prompt either repetition (inputting a similar thing more than once), or dissatisfaction (my character in diversion A will not work in amusement B). It would be an incredible change to take into consideration qualities to exchange, regardless of the possibility that not completely.

Insecurity: The existing Digital Identity Management systems are not secure and are prone to human mistakes. Users can pick weak passwords and thus compromise their systems.

## CONCLUSION AND RELATED WORK

With the development of Digital Identity Management Systems, users are able to access computer resources in various devices using same identity. This paper reviews existing digital identity management system models. Regulation of information in cases when the entities requiring access to it are both highly diverse and spread is among the most significant challenges to effective identity management. A variety of normal technical questions also faces the field, for example, the manner in which information in centralized and distributed databases can be controlled. In a bid to ensure that information related to authorization and authentication is up to date and dependable within an organization's systems of information, handling personnel has been a major concern of identity management systems. The Silo Model, User-Centric Identity Management Model, Centralized Identity Management Model, and Federated Identity Management Model are the major digital identity management systems that are in use today. The research has indicated that the current identity infrastructure is very unreliable. There is no standard for the design and development of the models to follow; registration and identification schemes vary wildly. Digital identity, even within one site or organization, does not usually last more than a fixed period of time. This makes the current digital identity management systems very insecure. The current identity management models are set up to allow for vast propagation of sensitive information. This leads to the discomfort of the user not knowing who possesses what information. In some instances, there is serious information leaks occur which can in turn lead to crimes such as identity theft. A hybrid digital Identity Management System model approach that will aim at solving the gaps identified in the existing digital identity models will be the future paper's subject of concern.

## References

Adjei, J. K., and Olesen, H. (2011). Analysis of Privacy-Enhancing Identity Management Systems. In Proceedings of WWRF Meeting.

Ahn, G. J., Ko, M., and Shehab, M. (2009, June). Privacy-enhanced usercentric identity management. In Communications, 2009. ICC'09. IEEE International Conference on (pp. 1-5). IEEE.

Albayan (2009) "ID Card cuts down process time to 7 seconds at Dubai Courts", Al Bayan Newspaper, [Online]. Website: www.albayan.ae. Issue date: 02 March 2009.

Alenezi, Hussain; Tarhini, Ali; Sharma, Sujeet Kumar (2015). "De-velopment of quantitative model to investigate the strategic relation-ship between information quality and e-government benefits". Trans-forming Government: People, Process and Policy. 9 (3): 324–351. doi:10.1108/TG-01-2015-0004. Retrieved 5 January 2016.

Allen, C. (1995) "Smart Cards Part of U.S. Effort in Move to Electronic Banking", Smart Card Technology International: The Global Journal of Advanced Card Technology, Townsendm R. (ed.), London: Global Projects Group

Barroso, L. A., Clidaras, J., and Holzle, U. (2013). The datacenter as a computer: An introduction to the design of warehouse-scale machines. Synthesis lectures on computer architecture, 8(3), 1-154.

Belanger, France, and Crossler, R. E. (2011). Privacy in the digital age: a review of information privacy research in information systems. MIS Q., 35(4), 1017–1042.

Bertino, E. (2010). "Digital Identity Management and Trust Negotiation," in Security for Web Services and Service-Oriented Architectures, Berlin, Springer

Camenisch, J. (2012). Information privacy?!. Computer networks, 56(18), 3834-3848.

Cavoukian, A., and Jonas, J. (2012). Privacy by design in the age of big data (pp. 1-17). Information and Privacy Commissioner of Ontario, Canada.

Coates, B.E. (2001) "SMART Government on Line, not in Line: Op-portunities, Challenges and Concerns for Public Leadership." The Public Manager, vol. 30, no. 4, pp. 37-40

Connolly, P. J. (2010). OAuth is the 'hottestthing'in identity manage-ment. eWeek, 27(9), 12-13

Donohue, M., and Carblanc, A. (2008). The role of digital identity management in the interneteconomy: a primer for policymakers. No. DSTI/ICCP/REG, 10.EUC Workshops, Denko, M. K., and International Federation for Information Processing

Fioravanti, F., and Nardelli, E. (2008). Identity Management for Egov-ernment Services. In Chen, (eds.). Digital government: e-government research, case studies andImplementation. (pp. 331-352). Berlin: Springer.

Guthery, S.B. and Jurgensen, T.M. (1998) SmartCard Developer's Kit. Macmillan Technical Publishing.

Hammer-Lahav, E. (2009, October 16). Beginner's Guide to OAuth – Part I: Overview.

Hovarka, D. Incommensurability and multi-paradigm grounding in de-sign science research: Implications for creating knowledge. In Human Benefit through the Diffusion of Information Systems Design Science Research, J. Pries-Heje, J. Venable, D. Bunker,N. Russo, and J. DeGross, Eds., vol. 318 of IFIP Advances in Information and Communication Technology. Springer Boston, 2010, pp. 13–27.

Jain Palvia, Shailendra. ”E-Government and E-Governance: Definitions/ Domain” (PDF). csi-sigegov.org. Computer Society of India. Retrieved 12 December 2016.

Jøsang, A., and Pope, S. (2005). User centric identity management. In AusCERT Asia Pacific Information Technology Security Conference (p. 77).

K. Peffers, T. Tuunanen, M. Rothenberger and S. Chatterjee. ”A De-sign Science Research Methodology for Information Systems Research.” Journal of Management Information Systems (2008) 24(3): 45-77.

Kothari, C. R. (2004). Research Methodology: Methods and Techniques (2nd ed.). Oxford University Press, Oxford.

Kumar, V., Mukerji, B., Irfan, B. and Ajax, P. (2007) Factors for Success-ful e-GovernmentAdoption: A Conceptual Framework. The Electronic Journal of e-Government, 5, 1, 63-77

L'Amrani, H., Berroukech, B. E., El Idrissi, Y. E. B., and Ajhoun, R. (2016, October). Identity management systems: Laws of identity for models 7 evaluation. In Information Science and Technology (CiSt), 2016 4th IEEE International Colloquium on (pp. 736-740). IEEE.

Lips, M., Taylor, J. A., and Economic and Social Research Council (Great Britain). (2007).Personal identification and identity management in new modes of e-government.

Mahler, T. (2010). Legal Risk Management Developing and Evaluating Elements of a Method for Proactive Legal Analyses, With a Particular Focus on Contracts. Monograph, The Faculty of Law, University of Oslo, Postboks, 6706.

Mangiuc, D. M. (2012). Cloud Identity and Access Management–A Model Proposal. Journal of Accounting and Management Information Systems, 11(3), 484–500.

Microsoft. (2011, February). Microsoft and U-Prove— End to End Trust — Microsoft TrustworthyComputing. MICROSOFT U-PROVE CTP RELEASE 2. Retrieved October 14,2012, from http://www.microsoft.com/mscorp/twc/endtoendtrust/vision/uprove.aspx

Shibboleth. (2013). Shibboleth - About. Retrieved January 10, 2013, fromhttp://shibboleth.net/about/index.html

Sismondo, S. (2011). An introduction to science and technology studies. John Wiley and Sons.

Thakur, M. A., and Gaikwad, R. (2015, January). User identity and Access Management trends in IT infrastructure-an overview. In Pervasive Computing (ICPC), 2015 International Conference on (pp. 1-4). IEEE.