JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

DIGITAL IDENTITY EVOLUTION AND SECURITY CHALLENGES

[1]Harshitha Sanaka, [2]Akshaya Padala, [3]Dr. T. Venkata Ramana

[1]Student, [2]Student, [3]Professor
[1,2,3]CSE Department,
[1,2,3]Sphoorthy Engineering College. Hyderabad, Telangana, India.

Abstract:

As the use of technology is growing and there is a huge growth in the use of digital operations. It is very important to prove yourself to achieve the economic, social, profession and personal development of the individuals. In the current generation, organizations or individuals need identity solutions which will be valid among different countries, states, organizations, technologies etc. To implement the secure identity solutions, revolutionary technologies like blockchain, Artificial Intelligence, IoT etc., are very helpful in providing secured identity services. Digital identity is the of identifying the individuals or devices with the help of digital process. With the help of different characteristics, features and other information which will be uniquely identifying the object. This paper presents the information related to digital identify evolution, importance, security challenges, comparative analysis, solutions, research gaps and conclusion.

Index Terms: **Digital identity, security, security challenges, digital signatures, cryptography.**

I. INTRODUCTION

Whenever we call to an organization or to a bank and request for the account information, then bank people will ask some queries which need to be answered for providing the identity of the individuals, this is nothing but the digital identity.

Evolution:

In the early days of using internet, ARPANET introduced the use of internet and stored the information of the users with the help of the database. Department of Défense has created the ARPANET and implemented the identification of the devices with the help of addressing mechanism. This addressing mechanism helps the devices to communicate with each other, to send and receive the information. This addressing is done by using the “Host names” mechanism, but this type of system is not worked in long run and avoided keeping the names to identify the device. Later on they invented the DNS (Domain Name System) which consists of protocol suit (TCP/IP) and served as one of the initiative step for achieving the digital identity.

Another way of achieving digital identity is implementing the public key cryptography. One of the mechanisms which implements the public key cryptography is digital signatures. If the user wants to send the information to the receiver, after receiving the same information by the receiver, he needs to prove that he is the intended receiver to receive, that is digital identity need to be achieved. This can be implemented by using the digital signatures where the message which want to send by the sender will be converted into cipher text by using a key, if the same key is there with the receiver, then only, he will be able to open the text and read it. That key helps the system to identify the receiver and this is one of the mechanisms of digital identity.

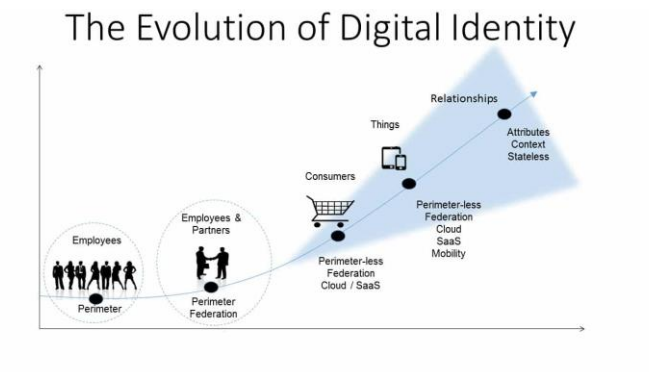
The Evolution of Digital Identity
Employees
Perimeter
Employees & Partners
Perimeter Federation
Consumers
Perimeter-less Federation Cloud / SaaS
Things
Perimeter-less Federation Cloud SaaS Mobility
Relationships
Attributes Context Stateless

Figure 1: Evolution of Digital Identity

Source: www.r3.com/blog/the-evolution-of-digital-identity/

As digital signature is one of the best solutions for digital identity, but still there is some issue like certificate authority which needs peoples trust for centralized solution. Because of this people are looking for another alternative digital identity solution which is known as

Context:

There are millions of data transferred every day through the internet. You are one of those who make such transactions each day. But how are you identified over that hefty data? These questions are answered by 'Digital identity'.

What do you understand by the term Digital Identity? Digital Identity refers to the information about you which is present online. Whenever you use personal information such as Username, password, DOB, Medical History etc., on the web, your digital identity is created. It authenticates your identity over digital channels through one of more factors like Fingerprints, Iris, Face, Voice, pin or password or with any other mechanism. This information is often used by the website owners to track the users for personalization and advertising.[1] Like the website, does anyone else track our data? How secure is our data online? These questions give rise to a new term 'Digital Security'. It encompasses tools used to protect one's digital identity using security elements such as passwords, anti-virus software.[2]. Because the websites take our personal information, Digital identity always comes along with privacy and security risks. People might always feel vulnerable to be storing their information while setting up the profiles in any new websites

Digital identity is a context where the thing which is represented with one or more features should be distinguished with the other things whether it may be device or individual. As per the ISO standards, digital identity refers that recognizing individual, objects, organization or any other devices with the help of their features distinctly with one another. One can use different attributes for identifying individuals, legal entities and for different types of assets. If we consider humans then we can consider age, height, date of birth and fingerprints, when we think about the legal entities then we can consider industry and business attributes, coming to the asset, we need to know the asset name and who is the issuer of the asset etc. All these attributes can be considered as inherent attributes which are intrinsic to an entity, they will not have any type of relationship with the external entities. There will be sone other attributes will be considered for the identity which includes accumulated attributes and assigned attributes. Accumulated attributes for the individuals include health records and individual behaviour data, for the legal entities business records and legal records, coming to the assets we can have ownership history and transaction history. Assigned attributes are given to the entity and may change over a period of time. For example, if we consider individuals then SSN, mobile number and mail id, for legal entities jurisdiction, directors etc, talking about the assets assigned attributes like custodianship and identifying the numbers.

II. RELATED WORK.

A. *Security challenges in Digital Identity:*

- Businesses need to practice best aspects of stopping hacking related issues which are associated with data protection. There are number of chances for getting attacked to malicious hacking issues.
- The old cloud security mechanisms are no longer involved in helping people to protect their data from external sources. The zero trust approach mechanisms have to be implemented in the organization for protecting data in the organization. [1]
- The contemporary issues are very high in application which are used by current organizations for protecting data. This data utilization have to be solved to great extent in order to overcome hybrid presentations of data.
- The IT security and IT admin are two important sources where equilibrium should be established between these two aspects. The IT admin is used in order to establish simple IT protection solutions. But in the recent days there is tremendous increase in data which is used by these business organizations because of which there is the need of taking IT security that can increase security of the organization. [2]
- The poorly maintained digital identities should be identified at the earliest as cyberattack criminals consider these poor digital identities as their favorite attacking sources. There is the need of implementing strong security systems which can reduce the effect attacks that could secure data used in the organizations. [3]
- Talking about Digital identity for public and private service access, Author Morten Meyerhof Nielsen [6] mentioned that the number of 60+ year old's will increase by the year 2050 and unemployment in youth will lead to limitations in the funds or public services. Technology driven efficiency and effectiveness in service production is one of the solutions to such challenges. When we are replacing humans with technology, Security to our personal information is the major issue. Digital identity and signature provide cost-effective, easy, secure, and personal service access. Most of the users would like to know when and what type of personal information is being collected when accessing digital services. Nielsen in their paper mentions that technology is secondary when compared to quality of data. Cooperation between authorities facilitates efficient and effective identity management, and partnerships with banking and telecom sectors can be very beneficial [6].

- Using the Internet, people are benefiting from accessing the vast amount of information quickly. Information can be of many forms like from paper transcripts to digital form of data which can be transferred using e-mails. Whatever form the information is, it must be protected. Information deriving from useful data is the main asset of any organization. As it is always easy for everybody to access, anyone can access it irrespective of whether they have good or bad intentions. Some of the most serious threats are listed below:

  - Deliberate software attacks.
  - Technical software or hardware failures and errors.
  - Acts of human errors or failures.
  - Deliberate acts of trespassing (unauthorized access).
  - Deliberate acts of Sabotage or Vandalism (Destruction of Information).
  - Deliberate acts of theft.
  - Compromises to intellectual property (piracy, copyright)
  - Quality of service devotions from service providers.
  - Technological obsolescences(outdated technology).
  - Deliberate acts of information extortion (blackmail for information disclosure).[6]

A. *Identity models:*

The following two are highly important identify models which need to be learned for data identification:

Conventional (Siloed) identity: This is the identity which is used from very long ago and major business groups use this data for preserving their customer information. The User ID will be given to customer with password. In this User ID entire information related to customer is stored. But it is not strong one breach can make entire customer data to get compromised because of external forces. In this way there will be thousands of customers data which may fall into danger with the usage of this conventional (Siloed) identity. [4] The e-commerce units use this model even after knowing it as risk because of the simple process which is associated in implementing this project. The cost factor also plays very important role in the implementation of this model. This is because it is less expensive compare to other software systems. This has led most of the business organizations to implement this model in operating there e-commerce systems. [5]

Federated identity and identity Providers: The federated identity approach should be implemented in the organization and it should be considered as safest mechanism in gathering information form customer. The login with google approach is the important aspect of this federated identity where users get good solutions for all their security related issues. The key functioning of this Federated Identity is avoiding duplication of identities which takes place in the organization. [6] The google identifies identity which is already recorded in the system. Once identity is created then no way same identity can be created in the system which gives wonderful protection to existing users in the system. The most important characteristic of this Federated Identity is gaining identity provider (IP). There is also the drawback which is associated with this Federated Identity as geographical issues are associated with this system. The Google search links are not available in certain areas because of which access to this system is not possible. [7]

C. Digital Identity Approaches:

In this section Bottom-Up approaches are dealt in order to understand decentralized digital system used for the purpose of verification. In digital signature and CA system one should identify that for the purpose of security CAs have made authorization of digital signature centralized. There is no chance of authorizing signatures by the common users in this commonly followed approach. In order to overcome process of centralization and establish decentralization Pretty Good Privacy was implemented. The main aim of this approach is to verify identity of other people by establishing trust. The development of trust between the uses is considered as the most important aspect of this Pretty Good Privacy. [8] In most of the cases getting knew about other people identity is very crucial in order to serve right business to those customers. Even at the time of making certain payment it is important for user to know about status of another person. The decentralized environment is the only way for achieving all these challenges associated with identification of right customer. But even this approach has certain limitations as emails which are floated through google and yahoo are highly centralized by these websites and making detailed analysis of in and out users sending this message is not at all possible. It should also be remembered that getting to know about information which is passes by users using these websites is not at all easy for common users who have limited knowledge on system securities. [9]

D. *Comparative Analysis*

The comparative analysis should be done between conventional identities and Federated Identity and Identity Providers. The conventional identities are not at all considered as best in comparison to Federated identities. In the conventional identities security is given only at the limited access level. That is a user can protect is user ID with appropriate password and login ID. The data protection is considered as very minute as any small link can make the data which is given by the customer go into compromise. The mechanism is used as it is very easy to implement in operations of the business. [10] On the other hand one should understand importance of federated mechanism as there are number of security benefits associated with this kind of mechanism. In federated identity one should know that systems are designed in such a way that proximity of data is no way possible. The system will not given any chance for their users to create proxy information that can harm trust of the users. The customer credentials once created cannot be created once again in the system. The chances of mis utilizing data can be achieved to great extent with this Federated Identity systems used in the organization. [11]

E. Research gaps

In the entire research analysis of data that is presented in this document one can say that there are certain drawbacks in both the models. The conventional model carrying its drawback and at the same time even Federated systems are carrying their drawbacks. The process of solving conventional system drawback should not be considered as very important as this is the system which may not be inexistence after few years.

This is because after few years every user who is associated with e-commerce will be knowing importance of security systems which have to be implemented in the organization. [12] The Federated Identity Systems have the major impact on the sending and receiving mails along with other identities. Once any identity is captured in federated systems and same cannot be copied by the other users. It means same identity can be given more than once in this federated system. That's the reason every users is interested in using these federated systems. If these federated systems are used in the high volume then data protection will be very easy for every e-commerce business. The only drawback associated with Federate systems is google and yahoo based systems cannot be used for the identification of data which is created earlier. [13]

III. CRITICAL REVIEW.

The most basic data storage systems were introduced in the internet at very early stages but later on it was decided to used best mechanisms in order to protect the data. APRANET and DNS are the only models which were used by early users. This has created lots of data storage issues for the users because of which new systems are implemented like siloed and aka Login with google. All these platforms have the feature of protecting data to fall into the hands of others. The prolific approach to check and knew about the users was achieved with new data protection mechanisms. [14] In most of the cases getting knew about other people identity is very crucial in order to serve right business to those customers. Even at the time of making certain payment it is important for user to know about status of other person. The challenges faced in system identity are solved with absolute ease with Federated System establishment. The credentials which are given to customers are neatly protected and perfectly encrypted to protect data from unauthorized users. In this way it can be said that when data is stored is database systems it should be protected with right system implementations.

The digital identity has made it very easier for people to access many things on the internet like in the E-Learning system. Such a system has availed everyone, equal opportunities to knowledge. This has made information reach at fingertip level, enabling the students to excel in studies. The biggest risk associated with digital identities is that of identity theft and misuse. We know that the creation of a digital identity usually involves using actual details about the person's real identity. Hence information in the wrong hands can be dangerous. Privacy risks and security threats are the primary causes of concern to be considered when it comes to creating a digital identity.

Many choose to create pseudonymous identities in a bid to disguise their real identities; while this might afford an added level of protection, experience proves that cross-site data analysis can be used to correctly isolate the real identity.[15]. In the real, offline world, identity cards and papers are issued only after a stringent verification process and exhaustive efforts are made to ensure that the subject's claims can be corroborated before any official identity markers are awarded to them. While a need for such a process for issuing digital identities has been recognized, it is practically unfeasible. Most people believe that using offline identity details to bolster a digital identity may actually do more harm than good since it exposes more of your real information.

At present, we are still to develop a standardized mechanism for authenticating digital identities fully and for preventing digital identity theft and misuse. The verification processes currently differ from platform to platform and depend on the purpose of the account/identity you're trying to create. For something as simple as an e-zine subscription, you might only need an email address, whereas for something a little more elaborate, such as an e-shopping website, you will have to tie your account to a physical address.[8]

Some platforms offer a greater level of security through mechanisms such as a two-factor authentication process. In these cases, you will usually have to include a second device, such as a mobile phone, in the process and you'll receive a digital verification code that you can then use to confirm your identity on the primary device/platform. For higher security services, consider investing in secondary digital security devices that use smart card technology and mechanisms like special access keys, call scramblers and smart SIMS to protect your phone number.[9]

On a personal level, caution and care are your greatest tools. Be careful where you supply your personal information and how much of it you're willing to hand out. Ask yourself if it's really needed and if not, are you willing to switch to a different platform? Whenever possible, stick to trusted platforms and service providers and exercise caution when asked to share any personal identifying information.

Digital ID offers individuals social, civic, and political benefits, from increased inclusion, formalization, and transparency to better control of online data. Designed carefully and scaled to high levels in multiple application areas, it can also create significant economic value, particularly in emerging economies, with benefits for both individuals and institutions. Yet with that potential comes risk from deliberate misuse of digital ID programs by government and commercial actors as well as broader risks common to other large-scale digital interactions, such as technology failure and security breaches. The design, governance, and use of digital ID is a rapidly evolving area deserving additional research. Topics for further investigation include system design, incorporating features to ensure fully informed consent both at sign-up and during ongoing usage; economic quantification of risks, encompassing design decisions and associated costs; relative benefits and downsides of different models for digital ID system governance and ownership—public or private as well as centralized, federated, or decentralized; and continued accumulation of an evidence base documenting benefits by use cases, including the link to specific design decisions and drivers of usage and adoption. While solutions are not always clear, and more research will help clarify upsides and downsides, digital ID is undoubtedly an important opportunity for economies, governments, businesses, and individuals around the world.

The policy landscape in a country will be important to set the framework for the ID system and as a means to address systemic risk. Multiple types of regulation may shape the way a digital ID system works. Legal protections and recognition for use of digital identity enable digital ID to serve its basic purpose. Data privacy policies establish the degree of individuals' control over their data as well as standards of care institutions must meet in handling individuals' data. Rules and regulations requiring individuals to show identification in order to receive products and services—such as KYC requirements to open financial services or telecom accounts—shape some of the ways digital ID can be used. On the flip side, if digital ID is used to satisfy such rules and regulations, it becomes all the more important to actively minimize the risks of excluding anyone who does not have, or does not want to use, a digital ID.

Governments, businesses, and civil society institutions can take action now as ID providers, requesting parties, users, and regulators Governments, businesses, and civil society actors will have to think through several important questions as they shape the course of digital ID programs in their countries, sectors, and communities. These include how to address potential misuse of the digital ID system, what may be an optimal approach to system design or a standard that can be developed regardless of varying country characteristics, and how to accelerate implementation and adoption. Some immediate steps that stakeholders can take to help capture the value of digital ID are outlined in this section. Governments can play the role of requesting party, for example by asking for information or authentication about constituents; ID provider, for example as the direct provider of a state-run system; or manager of a federated multiprovider system. In addition, governments will play critical roles as regulators and policy makers. In those roles, they can consider developing policies and legal frameworks to enable acceptance of digital identities, collaborating with international bodies to develop cross-border standardization, and partnering with private-sector institutions to understand country-specific economics of digital ID and to explore public-private and consortium-led models of provision. A business can be a requesting party, for example asking for information or authentication from a consumer or an employee; an ID provider, either as a stand-alone organization or as a member of a consortium; or both. Additionally, businesses can interact with digital ID regulation at the industry level by working on development of private-sector ID technology and implementation standards. Steps businesses can take include innovating processes that could leverage digital ID to boost efficiency and improve customer experience, working to facilitate development of global standards, and collaborating with governments to conduct bespoke cost-benefit analysis of digital identity and develop new digital ID programs. Civil society institutions can influence the priorities of businesses and government in the development of policy or program design. Steps they can take to help ensure that individuals capture the value of digital ID and to protect them from misuse include petitioning politicians, regulators, and institutions to develop digital ID programs and the policies necessary to make them safe, accessible, and socially beneficial.

Digital ID offers individuals social, civic, and political benefits, from increased inclusion, formalization, and transparency to better control of online data. Designed carefully and scaled to high levels in multiple application areas, it can also create significant economic value, particularly in emerging economies, with benefits for both individuals and institutions. Yet with that potential comes risk from deliberate misuse of digital ID programs by government and commercial actors as well as broader risks common to other large-scale digital interactions, such as technology failure and security breaches. The design, governance, and use of digital ID is a rapidly evolving area deserving additional research. Topics for further investigation include system design, incorporating features to ensure fully informed consent both at sign-up and during ongoing usage; economic quantification of risks, encompassing design decisions and associated costs; relative benefits and downsides of different models for digital ID system governance and ownership—public or private as well as centralized, federated, or decentralized; and continued accumulation of an evidence base documenting benefits by use cases, including the link to specific design decisions and drivers of usage and adoption. While solutions are not always clear, and more research will help clarify upsides and downsides, digital ID is undoubtedly an important opportunity for economies, governments, businesses, and individuals around the world.

IV. CONCLUSION.

The very first days of the "internet" introduced us to the most basic model of storing identities: the humble database. ARPANET, a precursor to the Internet created by the Department of Défense, involved each computer having a numeric address. It is clear that any kind of data that is stored in systems of database should be protected carefully with right kind of system solutions. If you want to make good use of the privileges provided by the digital identity you have to take some risk, and at the same time you should also make sure to follow some protocols to keep your digital identity safe and secure. The data protection mechanisms have to implemented at the higher level of system evaluations in order to identify any kind of misuses associated with data protection. More progress is needed to be done on Digital identity models if security is to be preserved throughout the data lifetime. We believe that the future of digital identity lies in giving individuals the control of their social presence

REFERENCES

[1] Beduschi, A. (2019). Digital identity: Contemporary challenges for data protection, privacy and non-discrimination rights. Big Data & Society, 6(2), 2053951719855091.

[2] Sathio, A. A., Dootio, M. A., Lakhan, A., ur Rehman, M., Pnhwar, A. O., & Sahito, M. A. (2021, August). Pervasive Futuristic Healthcare and Blockchain enabled Digital Identities-Challenges and Future Intensions. In 2021 International Conference on Computing, Electronics & Communications Engineering (iCCECE) (pp. 30-35). IEEE.

[3] Meyerhoff Nielsen, M. (2019, May). Tackling identity management, service delivery, and social security challenges: technology trends and partnership models. In 12th International Conference on Theory and Practice of Electronic Governance (ICEGOV2019). ACM Press.

[4] Barclay, I., Radha, S., Preece, A., Taylor, I., & Nabrzyski, J. (2020). Certifying provenance of scientific datasets with self-sovereign identity and verifiable credentials. arXiv preprint arXiv:2004.02796.

[5] Anand, N., & Brass, I. (2021). Responsible innovation for digital identity systems. Data & Policy, 3.

[6] Carretero, J., Izquierdo-Moreno, G., Vasile-Cabezas, M., & Garcia-Blas, J. (2018). Federated identity architecture of the European eID system. IEEE Access, 6, 75302-75326.

[7] Selvanathan, N., Jayakody, D., & Damjanovic-Behrendt, V. (2019, August). Federated identity management and interoperability for heterogeneous cloud platform ecosystems. In Proceedings of the 14th international conference on availability, reliability and security (pp. 1-7).

[8] Basney, J., Flanagan, H., Fleury, T., Gaynor, J., Koranda, S., & Oshrin, B. (2019, March). CILogon: Enabling federated identity and access management for scientific collaborations. In Proceedings of Science (Vol. 351, p. 031). Sissa Medialab Srl.

[9] Edris, E. K. K., Aiash, M., & Loo, J. K. K. (2020, April). The case for federated identity management in 5g communications. In 2020 Fifth International Conference on Fog and Mobile Edge Computing (FMEC) (pp. 120-127). IEEE.

[10] Duran, A., Pope, R. L., & Jones, S. R. (2020). The necessity of intersectionality as a framework to explore queer and trans student retention. Journal of College Student Retention: Research, Theory & Practice, 21(4), 520-543.

[11] Gray, C. M., Parsons, P., & Toombs, A. L. (2020). Building a holistic design identity through integrated studio education. In Educational Technology Beyond Content (pp. 43-55). Springer, Cham.

[12] Kapil, G., Agrawal, A., & Khan, R. A. (2019). Security challenges and precautionary measures: big data perspective. ICIC Express Lett, 12, 947-954.

[13] Sharma, K., & Gahlawat, M. (2021). SECURITY CHALLENGES IN BLOCKCHAIN BASED DIGITAL DOCUMENT VERIFICATION SOLUTIONS: A SURVEY. In CONFERENCE SECRETARIAT (p. 14).

[14] Paloque-Bergès, C., & Schafer, V. (2019). Arpanet (1969–2019). Internet Histories, 3(1), 1-14.

[15] Saxena, R. (2004), 'Security and online content management: balancing access and security', Breaking boundaries: integration and interoperability, 12th Biennial VALA Conference and Exhibition Victorian Association for Library Automation.

[16] Graf, F. (2002), 'Providing security for eLearning', Computers & Graphics, vol. 26, no. 2, pp.355-365

[17] Yong, J. (2007), 'Digital Identity Design and Privacy Preservation for e-Learning', Proceedings of the 2007 11th International Conference on Computer Supported Cooperative Work in Design, , pp. 858-863.