A COMPARATIVE STUDY OF TRADITIONAL AUTHENTICATION AND AUTHORIZATION METHODS WITH BLOCK CHAIN TECHNOLOGY FOR EGOVERNANCE SERVICES

RAMA YERRAMILLI,
9623421732, rama.y@nic.in

DR. NIRMALA KUMAR SWAMY,
9823120225, nirmalak@asmedu.org

ABSTRACT

With the increase in communication channels between various stakeholders in eGovernance scenario, offering secure e-Services by means of Authentication and Authorization became a crucial part. The multi factor authentication (MF) provides better protection effectively than the age old password based authentication. Governments are making efforts to establish multi factor authentication without comprising on provisioning the e-services. But there are some drawbacks in this centralised mode of authentication. In this paper, an exploratory comparative study of usability of blockchain technologies in eGovernance by studying National and International scenarios and the methods to provide e-services. Secondary data study will be conducted for studying the existing Authentication and Authorization of the user in e-services. The researcher is considering the factors like centralisation, scalability, trust factors while comparing various MF technologies and proposing usage of blockchain technology in eGovernance services by taking a case study of eHealth services.

KEY WORDS: Authorization, Authentication, 2 factor Authentication, Multi Factor Authentication, Blockchain

INTRODUCTION

eGovernance in the world is moving towards new era of good governance by establishing various communication channels with their stakeholders. The transactions are at varying risk levels and are exposed to the virtual world. So protecting privacy and securing the data are the main concerns while transacting in this digital environment. Deciding the level of risk on providing these services are also an important issue. Deciding the consumer of the service and also providing authority to use the service are also main challenges. Governments are framing their own policies and frameworks to establish the norms for authentication and authorization of the user.

Due to increase in hacktivism, governments are moving towards proactive approaches regarding cyber security and focusing on data protection. Governments are establishing multiple measures, framing rules and regulations and are pouring a lot of bucks on cyber security. Security concerns and measures are increasing and there by Governments need to create and improve sophisticated threat mechanisms. Going with the same security strategies cannot provide same level of results for providing security to the new age governance. Also, policies and mechanisms are getting established to increase in awareness regarding cyber security threats and preparing various methods and techniques to mitigate the threats.

Gartner defines “user authentication” as the real-time corroboration of a person’s claimed digital identity with an implied or notional level of trust.[1]

Authentication is the process of determining whether the claimed one is the same as they declared to be. Authentication will be followed by the rights to be provided to utilize the service which is called as authorization. New products and services are getting included in authentication market for enabling better implementation of authentication methods which are aiming at accompanying or removing the classical password bases authentication.

The main authentication methods are

- **SINGLE FACTOR AUTHENTICATION (THROUGH PASSWORDS) :**
  The most common form of Single factor authentication is password based authentication which has been in use since early days of computing. Passwords are indeed the weakest link in the security framework and in fastpaced environment, this security is not sufficient anymore.

- **2 FACTOR AUTHENTICATION :**
  2 factor authentication trends are increasing as it is easy to implement and use. It is just adding an extra step to the exiting authentication process (ie. password factor). It is often referred to a two step verification process in which the user provides two authentication factors. The usage of two factors is something he know and something he has (tools like OTP) or something he own (biometrics). Mostly this technology uses SMS based authentication and majorly used by financial applications. Major applications like eBanking, major government services along with Apple, Google and face book are implemented with this type of authentication. Still this technique is vulnerable as SMS-based authentication is being considered insecure as mobile network is more vulnerable. These 2 Factor mechanisms are largely used by financial institutions in worldwide.
- MULTI FACTOR AUTHENTICATION :
  Combination of any two or more factors will be considered in multi factor authentication. Password (and/or) Digital signature (and/or) one time password along with biometrics. A document with digital signature will be legally as valid as signed paper document. MFA creates a layered defence system against hackers to

break in since it is very hard to hack all the independent credentials like

- Something the user Knows (Password)
- Something the user has (software tokens)
- Something the user is (biometric verification)

In worldwide Google predictions in 2017 for the terms Single factor, 2 Factor and Multi factor authentication are mentioned below. [2]

- password based authentication is still stagnate
- Two factor authentication adoption will further increase
- Multi factor authentication didn't see abrupt increase as in the case of 2FA but it is a steady and rhythmic evolution.

- Still 2FA is not secure as the factors like SMS are traversing through insecure media like mobile networks. These systems are having a high risk of hacking as SMS can be easily intercepted by undesired parties.

General Landscape of the Authentication techniques in present world:

Governments are framing various policies and frameworks for authentication and authorisation in eGovernance services. Some examples are mentioned below.[3]

- United Kingdom (UK) Government – The UK Government uses a centralized registration and authentication system called "The Government Gateway" to support secure authenticated e-government transactions over the Internet. Authentication of customers (individuals, organizations or agents) is based on either a password or digital signatures (software tokens with password protection), depending on the type of transaction.
- gov.uk "Verify" is an identity assurance system developed by the UK government digital service (GDS)[14]. This system provides a single trusted login across UK government digital services. User can select a company among several designated companies (vendors) to verify their identity before accessing online eGovernment services. Around twelve online services are provided through this identity assurance system. Personal tax account, renewal of blue badge, checking income tax, checking state pension universal credit digital service, Self assessment of tax return, sharing of driving license information, claiming redundancy Payments, tax refunds and Rural payments. It is also used for reporting a medical condition which is effecting the driving. This system was made live in May 2016. Certified companies of this system verify identities at level 2. This level of identity assurance is sufficient to support a claim in civil court.
- Austrian Government – Austria uses the "Citizen Card" which is a device like smartcard, mobile phone, USB token, etc. This card is capable of creating secure digital signatures and can provide secure storage of personal data. Functions and data are protected by PIN against unauthorized usage.
- Danish Government – The Danish Government has taken initiatives to promote online eGovernance services to their citizens in the form of soft tokens in conjunction with the passwords. These are viewed as being secure enough at this stage for most public sector and private sector transactions.
- Estonian Government – The government of Estonia started distributing ID cards (personalized smartcards) to its citizens in January 2002. The cards contain the individual's name, address details, demographic information, as well as two PIN protected digital certificates and related cryptographic keys. Estonians can use their ID cards for accessing government services online and also e-commerce applications, with both authentication and digital signatures being supported (by the separate certificates). The authentication certificate contains the individual's email address. The ID cards are mandatory for citizens and permanent residents over the age of 15.
- Italian Government – The Italian Government system uses smart cards for citizen authentication and authorization services for online government services. These smart cards are named as National Services Card and Electronic ID card. Govt. is having plan to replace paper based IDs with these smart cards. The Electronic ID card is a hybrid smartcard that also contains PIN protected personal data including the holder's blood group and fingerprint scans.
- Malaysian Government – Malaysian Government issues MyKad or Government Multipurpose Card to all their citizens above 12 years of age. This is a tamper-resistant smartcard that performs public key cryptographic operations (including those relating to online authentication), supported by on-card digital certificates and a government Public Key Infrastructure. The MyKad is used for immigration at Malaysian borders, as a driving license, to access government services online, for making online purchases, as an e-purse, and as an ATM card with participating banks.
- Indian government established eauthentication and authorization policy regulations and also using several mechanisms for authentication and authorization. They are also provided single identity by using Aadhar card which is linked to many services to maintain unique identity of the citizens. As a part of eservice delivery, the Indian government also provided a guiding framework 'e_Pramaan' to all government ministries, departments and agencies for implementing the appropriate authentication processes and mechanisms. This also utilized for Aadhaar based biometric authentication while providing eauthentication mechanisms. This framework enables two way authentication. Depending on the risk level of the application, Indian government online services are authenticating using single factor mechanism, 2F mechanism and multi factor mechanisms[16].

UNDERLYING RESEARCH PROBLEM

In this scenarios explained above, 2way communication is getting improved and new channels of communications are getting opened between governments to citizens, governments to business. Authorization and authentication is the first building block for eGovernance structure. Authentication and authorization frameworks and policies are established at various levels in the world wide eGovernance. As economical applications are more and more penetrating in the day to day life of the citizen's life, like paying online taxes, ebanking, payment of fee or mainly day to day cash less transactions, risk levels are getting increased. With this, protecting the user credentials and transactions is becoming the crucial in eGovernance. In other way, from government side also it is becoming vital to identify and authorize the consumer of the service. Depending on the level of risk, different types of authentication and authorization mechanisms will be used. This can vary from single factor authentication to multi factor authentication. Technologies like single sign on, smart tokens and hard tokens and digital signatures are penetrating to establish more and more security. Also centralized mode of authentication and authorization techniques are getting penetrated in the world. Once if user gets authenticated, user can utilize any services with single sign-on. Cloud based solutions are also coming up. Centrally available Identity management service and data will increase the damage levels in case of comprising the sites. Is the centralized identity management trust worthy in the point of citizens?. Can Government services trust the user logged in centrally and provide the services with single sign-on ?. The cryptography planned today is enough for this cyber world where the crime rate is increasing ?. Is it a good idea to move from centralised to decentralised solutions for the above mentioned problem? Shall eGovernance move to trust-based centralized solutions to trust-free decentralized solutions?

So the researcher wants explore the blockchain smart contracts technology to mitigate egovernace identity management.

LITERATURE REVIEW

RELATED TO SINGLE FACTOR AUTHENTICATION :

Adams and Sasse [4] showed that, Security is not main concern of the users and then feel under attack by "capricious" password polices. Password policies often mandate the use of long (and hard-to-remember) passwords, frequent password changes, and using different passwords across different services. This ultimately drives the user to find the simplest password that barely complies with requirements[4].

RELATED TO 2F AUTHENTICATION:

Emiliano De Cristofaro, Honglu Du et.all did an exploratory study on the usability of the 2F technologies. They conducted a pre-study interview to identify the popular technologies and also the contexts and motivations for using the applications. They conducted survey based study on mechanical truck users. They used three metrics ease-of-use, required cognitive efforts and trustworthiness for their study and measured the usability of three popular 2F solutions. 1. Security tokens, one time pins received by email or SMS and dedicated smarphone apps like Google Authenticator).They find that 2F technologies are overall perceived are usable regardless of motivation and/or context of use[5].

RELATED TO MULTI FACTOR AUTHENTICATION :

Phillip H. Griffin described a method of authenticated key exchange (B-AKE) for achieving strong, multi factor and mutual authentication based on biometric based protocols. The protocol operations will relies on knowledge shared by communicating parties, extracted from data collected by biometric sensors. A Diffie-Hellman key-agreement scheme creates a symmetric encryption key using a weak secret, the extracted something-you-know data. This key protects the confidentiality of user credentials and other message data transferred during operation of the B-AKE protocol. If the message recipient possesses the same something-you-know information as the sender, a key is created, the message decrypted, and mutual authentication achieved. Biometric match data recovered from the encrypted message provides a second something-you-are authentication factor. The B-AKE protocol ensures users never reveal their knowledge or biometric credentials to imposter recipients or man-in-the-middle observers. Diffie-Hellman key establishment provides forward secrecy, a highly desirable protocol property, when participants choose fresh random values each time they operate the protocol[6].

Hassan Khan, Aaron Atwater, and Urs Hengartner did a comparative evaluation of implicit authentication schements.They collected six diverse IA schemes on four independent data sets over over 300 participants. They evaluated the parameters of these schemes in terms of: accuracy; training time and delay on real-world datasets; detection delay; processing and memory complexity for feature extraction, training and classification operations; vulnerability to mimic the attacks; and deployment issues on mobile platforms. They identified 1)promising IA schemes with high detection accuracy, low performance overhead, and near real-time detection delays, 2) Common pitfalls in contemporary IA evaluation methodology, and 3) Open challenges for IA research and finally provided an open source implementation of the IA schemes evaluated in this work that can be used for performance benchmarking by future IA research[7].

RELATED TO BLOCKCHAIN SMART CONTRACTS:

Jonathan Chester was discussed in his article about insecurities in 2F technologies and the threats on centralised storage of Identification data. He suggested combination of cryptographic hashing and blockchain technology[8].

Jacob stenum Czepluch et.all in their paper Blockchain- The gateway of trust-free cryptography, described blockchain as technology which provides distributed trust- free cryptographic systems. They followed design science approach and developed a proof of concept prototype which is having the potential to replace trust-based coffee shop payment solution which is based on an analogue, pre-paid punch card solution. They mentioned the benefits and limitations using the blockchain smart contracts. They are also mentioned the limitations and future developments required in blockchain technology as scalability, time and cost which the user needs to bear [9].

In many literatures blockchain technology is mentioned as the backbone technology behind Bitcoin. Blockchain technology was developed by ethereum in late 2013(Buterin 2013). Blockchain is not a new technology but it is a combination of known technologies applied in a new way. It is a combination of three technologies. Internet, private key cryptography and protocol governing incentivization. It has a great potential to transform multiple industries and make processes more democratic, secure, transparent, and efficient.

In financial sector the technology of blockchain become famous in the world. 90+ central banks are engaged in Blockchain discussions. Globally, 2500+ patents filed over the last three years and 80% of the banks predicted to initiate Blockchain and distributed ledger technology (DLT) projects by 2017[10].Other than financial service industries, even telecom, healthcare and life sciences, travel, hospitality and energy services are also moving close to implement the potential of blockchain technology by distrusting the traditional methods[10].

The implementation of Blockchain technology will leads to execute the transparent transactions in a quick and cost effect manner. Nowadays the entire world is paying attention towards Blockchain due to the decentralized technology with cryptographic implementation of security of transaction.

BLOCKCHAIN TECHNOLOGY:

A Blockchain is a digital, immutable, open, distributed ledger that chronologically records transactions in near real time. The prerequisite for each subsequent transaction will be added to the ledger in the respective consensus of the network participants (called nodes), thereby creating a continuous mechanism of control regarding manipulation, errors, and data quality. Blockchain is a protocol for exchanging value over the internet without an intermediary.

Merkle tree or hash tree is the technology used for block chain. As name says, Blockchain is a chain of blocks. It is the binary data structure with hash pointers. Each block contains the data of transactions within a period of time and a reference (hash value) to the block before. It is a distributed data structure where data blocks are grouped in pairs and the hash of each of these blocks is stored in a parent node. This grouping of hash codes continue till the root node. So tampering any block will lead to tampering all the preceding hashes till the root node. This makes this technology tamper proof. The another advantage is proof of membership. Due to Merkle tree properties, knowing the root member is enough to know all members in the tree. And also traversing through hash tree is faster than traditional binary tree.

- Types of block chains are :
  - Public blockchain: Public block chain is the open blockchain where anybody can read or write by showing proof of work.
  - Permissioned blockchain: Permissioned Blockchain has selective transparency with right access to selected nodes and provide consensus of the transaction.
  - Private blockchain : Private blockchain is a closed environment in which permitted users can only have rights to join the network.
- Blockchain key features are :
- Distributed ledger
- No intermediaries required
- Irreversibility and immutability
- Near real time
- Smart contracts: The smart contracts features is going to make new trends in Identity management system. Smart Contracts are stored procedures executed in a Blockchain to process pre-defined business steps and execute a commercially/legally enforceable transaction without the involvement of intermediary.
- The benefits of smart contracts
  - Sophisticated cryptographic authorization and verification mechanisms enable trust in shared data across complex multi-party network
  - Time stamping
  - Security
  - Authenticity

Table 1. In nutshell comparison for traditional methods of authentication with Blockchain smart contracts.

Traditional methods	Blockchain smartcontracts
Centralised Location	Distributed Networks
May not have history of transactions	Hyper Ledger technology
Cryptography should be enforced	Cryptography is incorporated in the technology itself.
Transactions will not have any link with the previous until it is programmed in such fashon.	As name says, each transaction will be stored as chain of blocks, each block called as nodes and each node will be linked with previous node with a hash value till root node.
Change in any transaction in middle is possible as transactions are not stored in tree structure	It is difficult to change any transaction because of cryptography and linkages with previous nodes.
System will fail in case of any server fails if disaster recovery is not properly planned	One node failure will not leads to system failures as it is distributed structure
Downtime will be more in case of server or network failures	Downtime will be less with distributed networks
The structure is closed and the issuer will only know the system	It is opaque and open to the user
It is scalable	Scalability is a problem
It is fast to transact	Time to mine a node may be more
Transaction cost will be barred by the service provider	Transaction cost needs to be barred by the user

BLOCK CHAIN TECHNOLOGY IN INTERNATIONAL EGOVERNANCE :

United states postal services are started using blockchain technology for their postal services[18]. The executive summary of US postal services described the implementation of blockchain technology in postal services and also explained the benefits. Their services are ranging from money-order and international money transfers. Additionally blockchain is an enabling technology that could allow the Postal Service to improve its operations and expand its services through emerging applications such as identity management and supply chain management. This summery examined the benefits and its potential impacts in using blockchain technology in postal services.

The US Postal Service experimented the blockchain technology with the financial applications. Their financial services like money transfers are improved by leveraging this technology. Because of this, implementation streamlined the back-end services which leads to a faster and cheaper service. Another service international money transfers also improved due to the technology's borderless nature.

In the long-term, Us postal service wants to expand their implementation to other non financial areas especially identity services, device management, and supply chain management.

So by looking at the implementation at the postal service which is a highly trusted government agency, block chain can be best suited for other eGovernance services also. Identity services are one of the biggest areas of opportunity in the blockchain community which would be well-suited for a role in identity verification.

DISCUSSION ON USAGE OF BLOCKCHAIN TECHNOLOGY IN EGOVERNANCE:

Worldwide, Governments are offering wide range of features and online services as mentioned above and trying hard to provide security and privacy of data that was getting gathered. Identity management and giving correct privileges to users are the major concerns in eGovernance. One government, one citizen with one identity is well suited phenomena for identity management as it can properly authenticate and authorize the user, and increases security levels. For achieving this features, wide variety of frameworks for authentication and authorizations, central location of identities, single gateways for authentication are getting established. But in case of hacktivism of the central location, the loss will be unpredictable and recovery from the loss is also huge. The centralized web based systems can't be verified by user and only issuer will have the right to do so. User has to trust the system that it works properly. And also dependency on reliability on hardware increases. Downtime is compulsory in case of hardware, network and software breakdowns. Taking regular and timely backups are very much required otherwise the loss of data and system is huge in case of system crashes. So the opaque, distributed, trust free, cryptographic features of block chain may solve the problem. If a node crashes, still the system will be up. No one can hack the transaction, as it is having the feature of grouping of nodes and hash mechanisms. Changing the hash value at one node is not possible to trace the transaction as it should traverse till root node to get the details of the transaction. Proof of membership is possible due to Merkle tree structure of blockchain. As the system runs transparently, the user need not trust the issuer also and so it becomes a trust- free solution.

Still this technology is having some shortcomings which needs to be addressed properly.

Scalability : For achieving the full fledged security of block chain, a larger number of nodes needs to be established. Otherwise the system will end up with less decentralised system like bitcoin experience(Hashrate 2015) which nullifies the main decentralized feature of blockchain. Ethereum has taken measures towards managing scalability issue faced by Bitcoin. Another solution is having many decentralized blockchain for specific purposes(Buterin 2014c). By establishing interconnectivity between different chains, security feature may be more increased. Another disadvantage of blockchain technology is time factor. And also the blockchain usage is not free of cost, the user needs to pay the cost for it. Still more understanding is required to conceptualize and use the full potential of blockchain technology. However by looking into the features of the blockchain technology, it may best suites future eGovernance economical and information systems.

Especially in Health care systems, where the privacy, security of patient information and other health related data, blockchain may open the doors for new secured, trust free management systems. As healthcare industry is moving away from paper-based medical records which are controlled by physical building structures and files, secured infrastructure which supports strong identity and security mechanism is required. Security and privacy of patient information, maintaining secured ledger of patients medical history, secure carrier for portable medical records, for reducing the healthcare fraud are main concerns in health care systems. The trust-free, decentralized, cryptographic blockchain mechanism may solve this problems. As no intermediate control will exists in the blcokchain technology, it becomes more and more trust-free solution.

For implementing health care patient management system, smart contacts needs to be implemented. Health card information will be replaced by digital smart contacts. Authentication and authorization will be created by providing functions while issuing the digital health cards. Authorizations and rights to utilize the services and insurance amounts can be calculated by established functions. Administrator will have the admin functions for setting the rules and maintaining the data. Functions for Online appointments, case histories, patient health records will be developed. Blockchain technology will create a chain of transactions of patients with cryptographic technique which leads to a foolproof system. The main limitations of blockchain like scalability also may be addressed by establishing multiple set of blockchains (block wise or sector wise). These multiple blockchains should be integrated so that the required health data will be made available to the systems like community health management systems used to estimate the disease rates and spread of communicable diseases. As multiple blockchains are established, the time for fetching the node is also will be less and time-factor limitation also gets solved. Maintenance of the system architecture becomes easy. Downtime will be less. Area wise management policies and regulations can be set easily. This may leads to high level security as data was distributed multiple locations and also scalability will increase.

REFERENCES:

1) https://www.gartner.com/doc/3210517/market-guide-user-authentication
2) https://blog.unloq.io/authentication-trends-for-2017-5f346a2c0823
3) https://www.ict.govt.nz/guidance-and-resources/ standards-compliance/authentication-standards/ guidance-on-multi-factor-identification/ government- use-of-multi-factor-authentication/
4) A. Adams and M. A. Sasse. Users are not the enemy.Communications of the ACM, 42(12), 1999.
5) A Comparative Usability Study of Two-Factor Authentication by Emiliano De Cristofaro†et.al
6) Phillip H Griffin : Biometric Knowledge Extraction for Multi-Factor Authentication and Key Exchange
7) A Comparative Evaluation of Implicit Authentication Schemes by Hassan Khan, Aaron Atwater, and Urs Hengartner
8) How The Blockchain Will Secure Your Online Identity, Jonathan Chester
9) BLOCKCHAIN – THE GATEWAY TO TRUST-FREE CRYPTOGRAPHIC TRANSACTIONS by Roman Beck, Jacob Stenum Czepluch, Nikolaj Lollike, Simon Malone
10) Blockchain technology in India Opportunities and challenges by delloide
11) DistributedCryptographyBased on the Proofs of Work By Marcin Andrychowicz and Stefan Dziembowski
12) On Trees, Chains and Fast Transactions in the Blockchain Aggelos Kiayias1 and Giorgos Panagiotakos
13) http://www.csoonline.com/article/3150997/security/what-2017-has-in-store-for-cybersecurity.html
14) https://www.rsa.com/en-us/blog/2017-09/top-5-authentication-trends-in-2017
15) https://blockgeeks.com/guides/what-isblockchain - technology/
16) Draft National e-Authentication Framework (NeAF) version 1.0 by NEGD,Govt. of India
17) https://en.wikipedia.org/wiki/GOV.UK_Verify
18) Blockchain Technology: Possibilities for the U.S. Postal Service RARC Report Report Number RARC-WP-16-011