Reinforce

The Apprentices of information technology from prominent academicians provide much needed reinforcement by publishing their research. The ideas presented here can motivate you to take up advanced research in the Information security domain.

---------- Reinforcing cyber security

- **Blockchain Technology for Cyber Security**
  --- P R Lakshmi Eshwari
- **Blockchain: Security Challenges**
  --- Ms. Bhagyashri Bhirud, Dr. Vinod Pachghare
- **Recent Developments in Intrusion Detection through Machine Learning**
  --- Nerella Sameera, M. Shashi

Blockchain Technology for Cyber Security

P R Lakshmi Eswari
Associate Director
Centre for Development of Advanced Computing (C-DAC), Hyderabad

What is Blockchain ?

Blockchain is an open, distributed ledger that can record transactions between different parties in time sequenced, verifiable and permanent way. Blockchain technology supports cryptographic guarantees of integrity and provides trust by signing every transaction. Through smart contracts the ledger can be programmed to trigger transactions automatically when certain predefined conditions are met. These features make blockchain data structure unique, overcoming the limitations of traditional databases. Any asset of value can be tracked and traded on a blockchain network, reducing risk & cutting costs for all involved. Asset can be tangible such as a house, land, vehicle etc., or intangible like patent, branding, trademark etc. Blockchain Technology has been around us for just near to a decade. Initially it was used for Bitcoin (which is a cryptocurrency, a form of electronic cash), but later people across the globe have realized its potential in other industries and various use cases have been initiated in e-Governance, Banking and Finance, Healthcare, Media, Smart cities, Judiciary, Insurance, Cyber Security and so on.

Why Blockchain Technology for Cyber Security ?

As the cyber security threats are becoming more sophisticated, researchers are continuously working towards designing advanced defense mechanisms using emerging technologies to protect computer systems, networks and the information from evolving threats. Blockchain Technology is found to be having good potential in cyber security domain due to its features such as enabling Trust, Transparency, Accountability, Auditability and Immutability. This technology helps in providing user identity management, transaction security, communication security, critical infrastructure protection and supply chain risk management. Blockchain technology can also play a vital role in enabling security and privacy aspects in IoT.

Global Initiatives:

Blockchain based PKI (Public Key Infrastructure)

In existing PKI systems, trust is enabled through either Web of Trust or Certification Authority (CA). Limitation of these PKI systems is that, Web of Trust is not scalable and CA is potential central point of failure.

Researchers felt that Blockchain with its implicit transparency and auditing features eliminates the need for central trusted third party. If PKI is maintained on a blockchain, single computer is replaced by a group of connected computers making it more robust and trustworthy. POMCOR, IOTA, CERTCOIN are some of the global initiatives in this direction.

Distributed DNS
Though DNSSEC enhances the security of DNS protocol, it does not address the issues such as DoS / DDoS attacks. Blockchain-based DNS alternatives, Namecoin and Blockstack are two initiatives to build decentralized and secure naming systems.

Anti Malware Solutions
BitAV is one of the anti-malware initiative, which is based on Distributed Blockchain Consensus and Feedforward Scanning. There are efforts towards building Blockchain based decentralized firewall for malware detection.

Protection from Supply Chain Attacks
Blockchain helps to design verifiable supply chains enabled with forensics to detect malicious activity, when we have dependence on foreign supply chains.

Logging and Integrity Management
Globally researchers are working towards logging and integrity management framework using Blockchain technology, which helps in providing assurance to end user especially in third party cloud service provider scenario. Audit trail for data transactions helps to detect data breaches and enables forensic analysis. Also detects malicious attacks such as code injections, APTs etc.

IoT Network
Blockchain technology can be used to track billions of connected devices in IoT networks, eliminating single point of failure. It enables decentralized security & privacy and more resilient environment for IoT devices to function in coordinated manner.

Blockchain : Security Challenges

Ms. Bhagyashri Bhirud
Department of Computer Engineering, College of Engineering, Pune

Dr. Vinod Pachghare
Department of Computer Engineering College of Engineering, Pune

The 'Blockchain' is a buzzword now-a-day. Initially, Bitcoin blew up tech-minds. Earlier people never realized that blockchain is the underlying technology for Bitcoin. Now people see blockchain as one of the robust, strong technology that is going to change completely the way things work today. Whether you work in finance, healthcare or real estate, you will probably be going to face blockchain in near future. After reading about blockchain, one might think whether it provides security to the application developed using the emerging technology or it's creating security challenges. Let's discuss the same in this article.

Introduction:

Blockchain is the chain of blocks. It was used to timestamp digital documents so that backdating or tampering can be avoided [2]. It was re-invented by Satoshi Nakamoto in 2008, to create digital cryptocurrency Bitcoin for which base technology is blockchain [5]. Figure 1 shows the flow of blockchain. Following four key components make it up for Blockchain [6]. Cryptographic hash functions and consensus helps in making the system tamperproof.

1. Shared Ledger
2. Cryptographic functions
3. Consensus
4. Smart Contracts

Blockchain is the distributed shared ledger that is open to anyone. It is like book-keeping of immutable transactions on a network. Each block contains data, the hash of that block and hash of the previous block.

Cryptographic hash functions are used for this. Data is something that is related to an application. Hash of a block identifies the block and is always unique. It is analogous to a fingerprint. Each block points to the previous block. The first block is called the Genesis block. When a block is created and is attached to the existing blockchain, the smart contract is run automatically. These are like real-world contracts however these are completely digital and immutable, stored inside a blockchain. It consists of rules, penalties and makes sure to enforce those automatically.
Being distributed, blockchain technology allows distributing authority instead of centralizing it. Instead of managing blockchain by the central authority, it uses a peer-to-peer network. The consensus is used to manage and maintain the reliability of data and transactions in a distributed network. In blockchain, four consensus methods are used [4]:

- PoW (Proof-of-Work) - It requires to solve a mathematical problem and arrive at a solution. The problem is computationally extensive, however, it's easy to verify once the answer has been reached.
- PoS (Proof of Stake) - This requires proving the ownership of the currency one holds with him/her. The person holding 5% of the currency, can mine only 5% of the blocks.
- PBFT (Practical Byzantine Fault Tolerance) - It is the protocol to tolerate Byzantine faults. The process works in three phases, pre-prepared, prepared and commit. At a phase, if ⅔ of nodes give a vote, then it allowed to enter next phase [4].
- DPoS (Delegated Proof of Stake) - It is like PoS, the difference is that the stakeholders elect their delegates. They, then, generate and validate the block.

Security Challenges:

Blockchain is developed using different technology infrastructure, techniques. This might lead to different vulnerabilities. Fol-

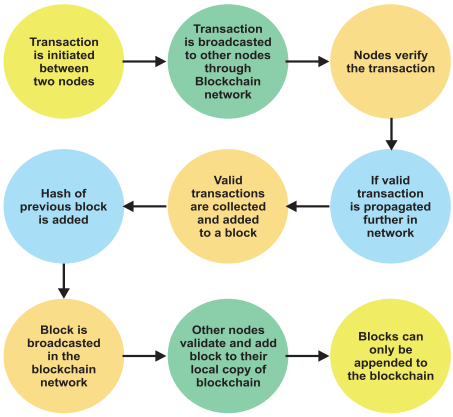
lowing are vulnerabilities and attacks that have been performed.

Vulnerabilities:

- 51% vulnerability - This is the vulnerability present in Proof-of-Work consensus protocol. If 'mining-pools' are created, they can acquire more than 50% of the total network power. Resulting in them controlling the blockchain [3].
- Private key security - In blockchain, a user's private key is generated by the user. It is not maintained by the third party. It's possible to crack a user's private key, which will result in exploiting and misusing users' identity and credentials [3].
- Double spending - It is simply spending the digital currency twice. It is not there in case of physical currency. In the case of digital currency, it is as easy as copying a file on a personal computer.
- Vulnerabilities in smart contracts - There are few vulnerabilities discussed in [3]
  - Transaction-ordering dependence
  - Timestamp dependence
  - Mishandled exceptions
  - Re-entrancy vulnerability
- Under-optimized smart contracts - There are few patterns which may give an opportunity to attackers to exploit [1].
  - Dead code
  - Opaque predicate
  - Expensive operations in loop
  - Loop fusion

Attacks:

- DAO - In June 2016, DAO smart contract was attacked. Attackers exploited a recursive calling vulnerability. DAO smart contract was deployed in Ethereum in May 2016.
- Selfish Miner - When a new block is discovered, it should be published to the network. However, selfish miners keep such new blocks to themselves and mine the further blocks. While honest miners keep on mining for already discovered blocks. Selfish miners thereby get rewards wasting the honest miners' computing power.
- Eclipse Miner - Eclipse miner gains control over a node's access to information in a peer-to-peer network. Then the attacker can eclipse the node so that it communicates with malicious nodes.
- Fork Problems - A fork is a change to protocol or divergence from the previous version. Hard forks are the deliberate ones, occurring when the community differs in opinions. Soft forks are optional, and users can keep running an old version.
- King of the ether throne - In this attack, out-of-gas send exception disorder was exploited.



Conclusion:

We discussed the basics of blockchain. Basically, it's based on, shared ledger, cryptographic function, consensus, and smart contracts. The cryptographic functions and consensus mechanism make blockchain secure. However, different vulnerabilities might arise through different causes like consensus mechanism, a public-key encryption scheme, transaction verification mechanism, program writing, and design flaws. Though basic security measures are considered while designing blockchain technology, the supporting technologies and interfaces might have flaws which creates different doors open for attackers.

Acknowledgement:

We would like to extend our gratitude towards ISEA for giving us the opportunity to help create awareness about cyber security. I would also like to extend my sincere thanks to Dr. Vinod Pachghare for his support, guidance.

References:

- *Chen Ting, X. L. (2017). Under-optimized smart contracts devour your money. In Software Analysis, Evolution and Reengineering (SANER), 2017 IEEE 24th International Conference on, pp. 442-446. IEEE, 2017*
- *Kerim, S. (n.d.). Is Blockchain a Rapper? Retrieved from Elpassion: https://blog.elpassion.com/is-blockchain-a-rapper-3f71c336f7b1?gi=af05648baed2*
- *Li Xiaoqi, P. J. (2017). A survey on the security of blockchain systems. Future Generation Computer Systems (2017)*
- *Zheng Zibin, S. X.-N. (2016). Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services 1 (2016): 1-25*
- *Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008)*
- *Gupta, Manav. "Blockchain for dummies." IBM Limited Edition, US (2017)*

Wht is Cryptocurrency mining ?

Cryptocurrency mining, or crypto-mining, is a process in which transactions for various forms of crypto-currency are verified and added to the blockchain digital ledger

Recent Developments in Intrusion Detection through Machine Learning

Nerella Sameera
Research Scholar, Dept. of CS&SE, Andhra University College of Engineering(A)

M. Shashi
Cheif Investigator of ISEA and Profeesor, Dept. of CS&SE, Andhra University College of Engineering(A)

Protecting the cyber space from vulnerability exploitation is the most difficult and challenging task. Sophisticated detection mechanism should be adopted for intrusion detection in-order to fight against the ever evolving attacks. This article describes the new developments like "Intrusion Detection System (IDS)", "Intrusion Detection Network (IDN)" and "Transfer Learning (TL)" in the field of cyber security and also covers various facets of cyber security and cyber intrusions. IDSs are the systems which can detect zero-day attacks but results in high false positive rates (FPR).

Knowledge sharing through IDN and model refinement through TL offer promising solutions to overcome the challenge. Different collaborative IDSs formed as a network for sharing attack knowledge constitute an IDN that can make more effective detection. However some of the nodes become victims of zero-day attacks leading to some FPR. TL offers promising solutions to handle this problem. TL is a recent advancement of machine learning that builds models for target domains with minimal or no labeled training examples leveraging the knowledge learnt from a related source domain having abundant training examples.

Protecting the cyber space from vulnerability exploitation is the most difficult and important task. This task of cyber security is challenging because of the ever evolving attacks emerging with greater speed of technological developments. Specifically three factors namely system, data and human errors are becoming vulnerable points and open the door for cyber-crimes. Victim's system infrastructure may contain some loopholes which may become vulnerable points. Some-times data itself may contain some hidden intrusions. Human-beings because of their bad cyber-culture like writing passwords on a paper, clicking on in-secure links or by giving all permissions while downloading apps, etc.., introduce vulnerable points. These factors results in different types of cyber intrusions. Viruses, worms, trojans, rootkit and spyware belong to the malware family. Malware replication, botnet, vulnerability exploitation, password guessing and phishing are the different attack methods. Denial of service (DoS) attack and web based attacks like DNS spoofing, SQL injection and XSS are the other types of cyber intrusions [1].

Highly sophisticated detection mechanism should be adopted for intrusion detection in-order to fight against these cyber intrusions. Intrusion Detection Systems (IDSs) are the software or hardware systems that monitor the network traffic and generate an alert to the system administrator upon detecting an intrusion. There are two types of IDSs [2]. One is Host based IDS (HIDS) that monitors only the activities of a single host and the other one is Network based IDS (NIDS) that monitors the activities of an entire network for detecting intrusions. IDS follow two detection strategies. One is signature or misuse based strategy to detect intrusions by matching the signature of the incoming packet with the existing attack signatures. In order to generate attack signatures, IDS involves analysis of extensive amounts of data for extracting hidden patterns and features in the form of signatures and hence calls for Machine Learning techniques which builds a model by considering the available data known as training data set and the model performance is assessed on testing data set. Once finalized, this model is used for detection of labels (attack or normal) for the new data. The assumption of machine learning algorithms is that the training and testing data are taken from the same domain so that input features and data distributions are the same. However, this assumption may not hold for the real world attack scenario with evolving attack patterns as the data distributions and features may change and deviate from those used in the construction of the model. This results in limited applicability of the constructed models for detecting zero-day attacks. Hence the signature based strategy is inefficient for detecting new attacks referred to as zero-day attacks due to lack of knowledge on the new attack signatures.

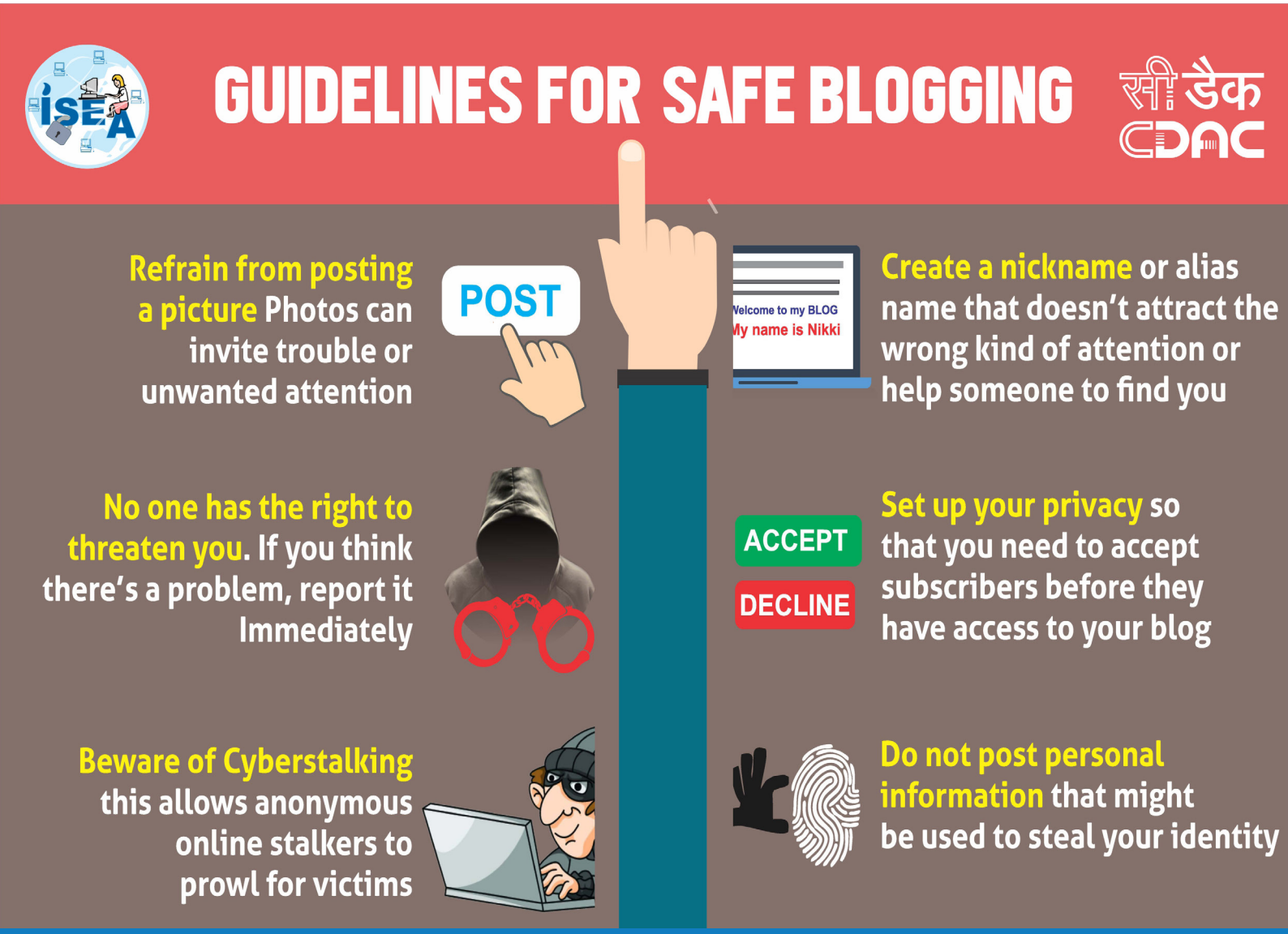
The alternative approach is anomaly based detection which can detect intrusions by observing the deviation of the packet's signature from the normal behavior pattern. This strategy can detect zero-day attacks but results in high false positive rates (FPR) leading to false alarms. Knowledge sharing through Intrusion Detection Network (IDN) [1] and model refinement with minimum labeled data through Transfer Learning (TL) [3] offer promising solutions to overcome the challenge.

One or more independent IDSs experiencing a zero-day attack may perform better with reduced false positive rate by information sharing through collaborative learning in Intrusion Detection Networks (IDNs). Different collaborative IDSs formed as a network for sharing attack knowledge constitute an IDN [1]. IDN allows each IDS to share attack knowledge with other IDS so that combining the information from multiple detectors might be helpful in increasing the detection accuracy. IDN follows two architectures. One is centralized, in which there exist central IDS that gathers, maintains and disseminates latest attack information for improved ability to make more accurate judgments about attacks identification. However, the centralized architecture suffers from reduced reliability due to single point of failure on the central IDS. The second architecture is decentralized where IDSs at all nodes participate equally in knowledge sharing and analysis. The IDNs aims to reduce the FPR while dealing with zero-day attacks by reducing the latency in formation and dissemination of signature of new attacks through knowledge sharing. However some of the nodes become victims of zero-day attacks unless they rely on hybrid architecture which includes signature based as well as anomaly based detection methods leading to some FPR.Transfer learning [3] offers promising

solutions to handle this problem. TL is a recent advancement of machine learning that builds models for target domains with minimal or no labeled training examples leveraging the knowledge learnt from a related source domain having abundant training examples [4]. Researchers proved that performance of the models built using TL is on par with models built by traditional machine learning algorithms even if the TL was provided with only one to ten persent of the labelled training examples. When applied to IDS, transfer learning handles the differences in feature spaces, marginal probability distributions with class labels among the attacks whose signatures are already captured and the new zero-day attacks whose signatures are to be captured with minimal or no labelled examples describing them. So with the help of TL, model constructed on related source domain can be refined for detection of labels (attack or normal) for the new domain (target domain) even though it (new domain) may have a different scenario, thereby increasing the detection accuracy of emerging intrusions with reduced FPR. HeTL [3], HeMap [5], Manifold Alignment [6] are the examples of different transfer learning algorithms. For detection of emerging intrusions, these algorithms transforms source and target data into a common latent space that preserves the original structure of the data, while at the same time, maximizing the similarity between the two. Later these projected data are used for model building on source data which will be refined appropriately to detect even zero-day attacks with high accuracy.

References:

- *Fung, Carol, and Raouf Boutaba. Intrusion Detection Networks: A Key to Collaborative Security. Auerbach Publications, 2013.*
- *Buczak, Anna L., and Erhan Guven. "A survey of data mining and machine learning methods for cyber security intrusion detection." IEEE Communications Surveys & Tutorials 18.2 (2016): 1153-1176.*
- *Zhao, Juan, Sachin Shetty, and Jan Wei Pan. "Feature-based transfer learning for network security." Military Communications Conference (MILCOM), MILCOM 2017-2017 IEEE. IEEE, 2017.*
- *Weiss, Karl, Taghi M. Khoshgoftaar, and DingDing Wang. "A survey of transfer learning." Journal of Big Data 3.1 (2016): 9.*
- *Shi, Xiaoxiao, et al. "Transfer learning on heterogenous feature spaces via spectral transformation." Data Mining (ICDM), 2010 IEEE 10th International Conference on. IEEE, 2010.*
- *Zahra Taghiyarrenani, Ali Fanian, Ehsan Mahdavi, Abdolreza Mirzaei and Hamed Farsi. "Transfer Learning based Intrusion Detection." 8th International Conference on Computer and Knowledge Engineering,2018.*

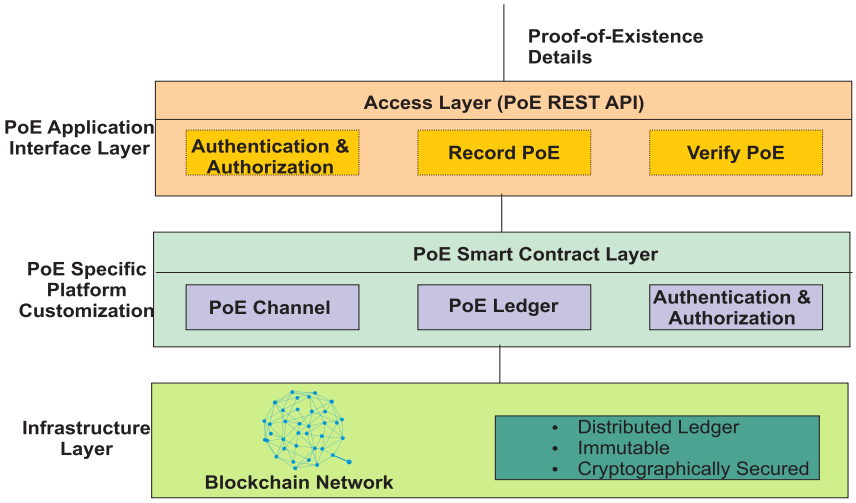


Blockchain based Proof of Existence as a Service (PoEaaS)

What is Proof Of Existence (PoE)?

PoE calculates the cryptographic digest of digital artefact and stores in the Blockchain along with the timestamp. It allows verifying the existence of digital artefact's hash on the blockchain. This proves the existence of digital artefact at a point of time when it was recorded on blockchain.

Architecture



C-DAC Blockchain based Proof Of Existence(PoE) Platform

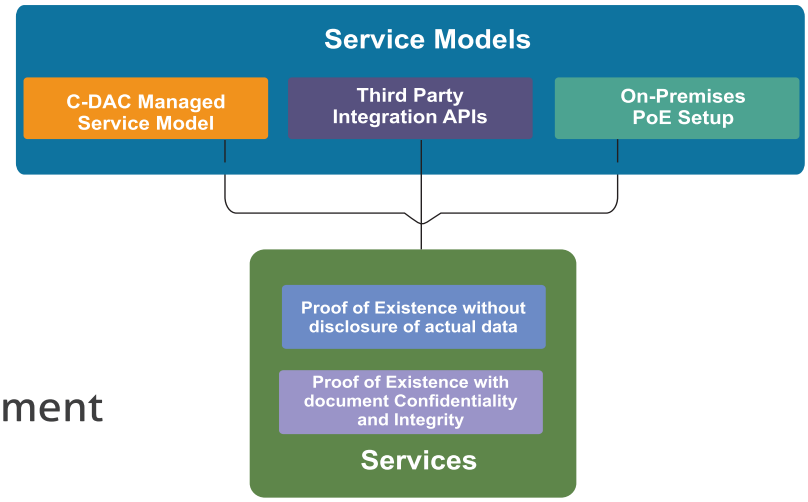
Benefits of PoE

1. Proves document Ownership without revealing actual data
2. Record time stamp & proves digital artefact exists at a certain moment of time
3. Certify the existence of document without the need of a Central Authority
4. Ensures document Integrity
5. Ensures that timestamp and hash of the documents cannot be tampered retroactively

Potential Use Cases of PoE

- Educational Applications
- MoUs / Agreements
- Driving Licenses
- Birth / Death Certificates,
- Sale Deed and Land Records
- Health Records
- Employee Service Records
- Log Management
- Enterprise Document Management
- And many more .....

PoE Service Models



For demo and queries mail us at cdacchain@cdac.in

प्रगत संगणन विकास केन्द्र
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING
इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय की वैज्ञानिक संस्था, भारत सरकार
A Scientific Society of the Ministry of Electronics and Information Technology, Government of India
Plot No. 6 & 7, Hardware Park, Sy No. 1/1, Srisailam Highway, Pahadi Shareef Via (Keshavagiri Post)
Hyderabad - 501510