ISSN (Online) 2456 -1304

International Journal of Science, Engineering and Management (IJSEM)
Vol 4, Issue 10, October 2019

Keyless Signature Infrastructure for Digital India's Security

[1] Mridul Sharma, [2]Rupali Sharma
[1][2] University Institute of Engineering, Rayat Bahra University, Mohali, Punjab, India

***Abstract*— In the making of new Digital India there are lots of threats which are there in the path of this dream. Acts of data breach of AADHAAR and Bank Accounts due to the lack of security in our digital services are common but the world is now, moving towards digital era so to be with the world in this digital transformation we must work on our security enhancement to provide a secure platform to government organisations. To serve the three aspects of security that is confidentiality, integrity, and availability of data we need an infrastructure that ensures all these. The Blockchain-Based KSI is the new technology which will support the government of India to achieve its goal of ensuring secure digital Services. It will help the government in providing strong authentication through digital signatures, and will also give the citizens a trust that their PII data is secure and confidential so that they can use these digital services for their all daily work. On the inspiration from Estonia where all their government services are digital in a way such that every government work from issuing a birth certificate to passport verification all these tasks are done digitally. This paper is made to help India in the implementation of this powerful Infrastructure for the digital governmental services providing ease to people and bureaucrats.**

***Index Terms*— Keyless Signature Infrastructure, Aadhaar, Blockchain and Personally identifiable information.**

I. INTRODUCTION

In today's world India is an emerging economy and the country as a whole has huge aspirations to get digitalized. But before we see this dream fulfilled there are multiple hurdles we would face along the way. We need to help India become a digital superpower, to overcome these problems and make this dream come true. One of the examples that come, at first sight, is how there is no centralized system for authorization of data in place. We also see the practices we use for the transmission of government data including data amongst banks is not up to the mark. We do see some flaws which can lead to attacks, some follies are being highlighted on the news every day. This research paper has been written by us to cover these security breaches. It shows the entire architecture of how we can secure our digital space by using an infrastructure that is hack-proof while not only transmitting and receiving the data seamlessly but also with hundred percent integrity.

A KSI infrastructure can help us build this kind of infrastructure. We see that the various major departments in the Government of India including most banks are using the public key Infrastructure for encryption. This makes the public key a high-risk item. A hacker can hack the private keys and decrypts the data. We have seen our AADHAAR database and various frontend servers easily hacked after theft of the private key by the attackers.

As we all know that data is the new oil, and for a nation to safeguard his data and PII information of 1.3 billion Indians is the first and top most priority. The size and volume of this sensitive information in itself increases the chances of this vulnerable data to be compromised at various levels. This paper focuses on what is KSI and how it works. It also showcases case scenarios to implement this in India on a national level. The scenarios are built along with the risks in our existing system and ways to mitigate them.

II. INFRASTRUCTURE OVERVIEW OF KSI

Keyless Signature Infrastructure is created by Guardtime in 2007 and implemented in Estonia. Keyless signatures are an alternative solution to traditional PKI signatures. It helps us to mitigate the risks in the traditional PKI infrastructure for the Integrity of data. The traditional PKI signatures may be protected by timestamps, but as long as the time-stamping technology itself is PKI-based, the problem of key compromise is still not solved. In KSI, there are multiple signatures (in other words, many documents are signed at a time.)

The Signing process consists of three major steps:

- Hashing
- Aggregations
- Publisher

Hash Tree-The hash aggregation was purposed by Merkle and called a Merkle tree. In this, the hash of the documents is combining to form a large hash tree. At the top of the hash tree there are the unique hash values. The user sends the hash of the document via the gateway to the aggregator servers and receives a signature token as a proof that data is

All Rights Reserved © 2019 IJSEM

ISSN (Online) 2456 -1304

International Journal of Science, Engineering and Management (IJSEM)
Vol 4, Issue 10, October 2019

present at that time and that request is coming from a specific access point. The signature tokens have enough data to reconstruct the hash tree via the reverse path flow, i.e. via the top hash value.

To verify this, we can take the x1 x2 x3 and x4 are the last leaves of the hash tree to check and verify the signature token of x2 so we replace it with y as a token of x2

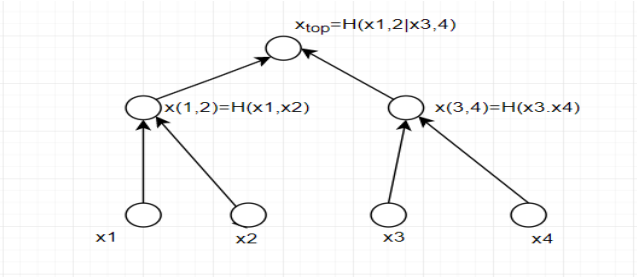

Fig. 1. Computation of a hash tree.

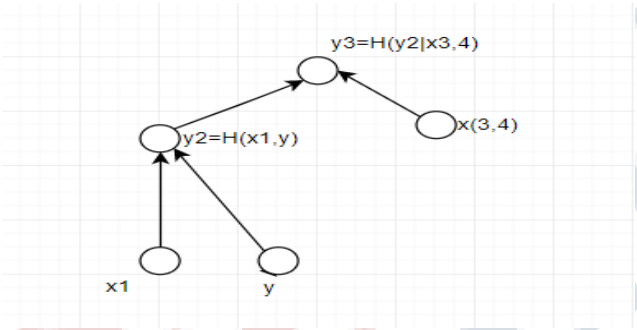

Fig.2. Verification of y token at the position of x2.

Hashing Calendar- The top values of the hash of aggregator servers are combing in a global hash tree called hash calendar which is globally available to all for the verification of issued signature token. Also, there is an algorithm to extract time value from the shape of the linking hash tree for each second, giving a hard-to-modify time value for each issued token.

Aggregation- A temporary global tree which is directly connected with the user applications via gateways to capture the hash value of user data and then this data forwarded to the upstream aggregation servers. The aggregation tree is horizontally split into four layers, and an infrastructure is built so that the top layer is adjacent to the core cluster; two intermediate layers provide geographic scale. The bottom layer is bundled with gateways and hosted close to end-users. Each aggregator labels its downstream clients by hashing their names into the hash trees. These forward secure labels form a hierarchical namespace used to identify distinct service end-points. The signature token with the timestamp is also sent back to the user by the aggregation gateways.

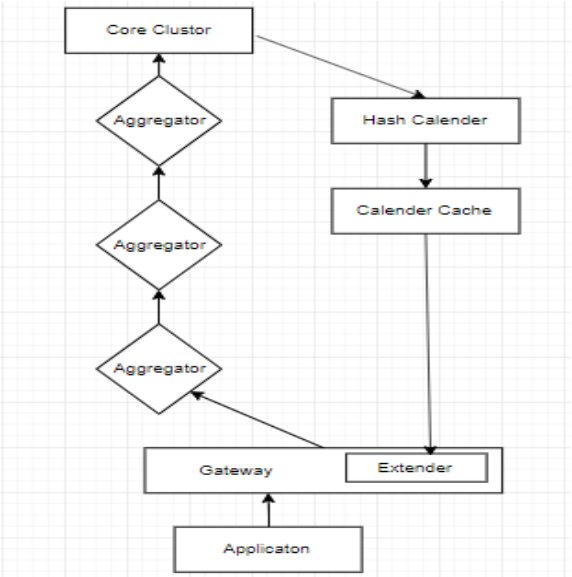

Fig. 3. Architecture of Aggregation Networks.

Publisher - The topmost hash value which comes from the aggregation hash trees to core cluster and making a hash calendar and that top hash value will be published as a trust anchor.

Core cluster- This lies above the aggregator network and its work is to store the top value of each aggregation server while also storing it into the hash calendar along with the timestamp for issuing the signature token.

Gateways- The gateway acts as an adapter which receives the inputs from the user in specific formats (RFC3161 and Open KSI) and then sends that request to its assigned aggregator. Another work of the gateway is that it acts as a verifier also (and is also called extender.) This means it can give the client a timestamped token from the hash calendar.

III. IMPLEMENTATION OF KSI WITH EXISTING INFRASTRUCTURE

We can implement this Infrastructure also with the existing infra as now we are using 2048-bit PKI mechanism in which there are sharing of keys. PKI signature is protected with the timestamps but the timestamping mechanism is also PKI based so there are lots of keys which needs to be exchanged and hence the risk of key theft increases. So, if we don't want to fully change our existing infrastructure, we can use this KSI based signature

All Rights Reserved © 2019 IJSEM

for the timestamping purpose. By doing this we will ensure that the integrity of data is maintained and its verification. The blockchain based technique will provide the extra layer of security in our existing architecture. It is a light weight technique. The small signature tokens with the timestamps of size 2-4 KB are generated per-round. The calendar database growth linear with time and this database is also not too large.

.

IV. EXISTING FLAWS IN OUR SYSTEMS

AADHAAR - the world's largest nationwide identity project which has all the PII data of 1.3 billion people including their banks account details and many more services linked to it - we see a report of a breach on this almost daily on the news. The admins are unaware or unable to see a threat. The AADHAAR website displays that it uses the 2048-bit PKI mechanism as security. And with the integration of AADHAAR with many government projects including banks, there are huge chances of theft of keys. This will help the attacker to decrypt the data of all the billion users and that is a huge number. Another example we can take is the UPI, a brainchild of the NPCI which is approved by RBI, also uses PKI mechanism. This system is further integrated with many mobile wallets. Thus, it's easy for the attacker to modify the API calls which happens between these platforms. This shows its vulnerability. So, when the volume of data is huge and the data is also PII sensitive it is our responsibility to use an infrastructure which is best in the world. Hence, KSI is the best alternative to the traditional PKI infrastructure. If we can implement this with the existing system, this blockchain-based KSI system will help us in many ways just like Estonia. By integrating all the government departments and their servers online we also reduce the chances of corruption, the availability of data is more and the integrity of confidential data would be maintained and the existing flaws can be corrected.

V. CONCLUSION & FUTURE WORK

The blockchain based KSI is the new emerging technology which has a limited audience but its more secure than the traditional methods. As implemented by the Estonian government for the official use we can also use it and provide the transparency of the data with the more secure methods. This paper reviewed the KSI technology that will enhance the integrity availability and confidentially of data if uses in the best possible way. It will fulfil India's dream of a fully digital nation. An infrastructure should be built that would help in implementing secure data transfers. In The next follow up papers will present a detailed roadmap of implementation of the infrastructure called X-road in India that will outline KSI and the path to follow so as to achieve an entirely secure digitalized infrastructure for Digital India.

REFERENCES

[1] Procedural Guidelines for UPI – NPCI, www.npci.org.in/sites/default/files/UPI-PG-RBI_Final.pdf December, 2016.
[2] Ahto Buldas1,2 , Andres Kroonmaa1 , and Risto Laanoja: Keyless Signatures' Infrastructure: How to Build Global Distributed Hash-Trees.
[3] Keyless Signature Infrastructure, https: //www. guardtime -federal.com/ksi/
[4] Trusted time stamping, https:// en. wikipedia. org/wiki/Trusted_ timestamping
[5] Vikash Chourasia: Public Key Infrastructure & eSign in India
[6] Randy D Bishop: Introduction to Guardtime and KSI Blockchain.

All Rights Reserved © 2019 IJSEM