Identity-Based Network Security for Commercial Blockchain Services

G. Bhuvaneshwari [#1],Mrs. M.kayalvizhi MCA.,M.Phil.,Ph.D., [#3]

Pg Scholar, Associate Professor &DSCASW College

Department of MCA &Dhanalakshmi Srinivasan College of Arts and Science for Women's- Perambalur, Tamilnadu, India

[1] revathimca97@gmail.com, [2] vizhimca@gmail.com

Abstract

While blockchain services hold nice promise to boost many alternative industries, there area unit importantcybersecurity issues that should be self-addressed.In this project, we present experimental test bed results for a novel method of user identity management for cloud-based blockchain applications.Using a BlackRidge Technology end point on a Windows host, we tend to insert cryptologic identity tokens on the primary packet to request a brand new session.A corresponding entree appliance within the cloud enforces security policy, obstruction unauthorized access at or below the transport layer.Results of penetration testing a sample Hyperledger 1.0 application are discussed.We conjointly demonstrate network segmentation and trafficseparation, that permits multiple organizations to share blockchain infrastructure and facilitates compliance auditing.

Keywords: Blockchain, cybersecurity, identity, authentication, hyperledger, cloud

INTRODUCTION

The use of blockchain technologies to supply changelesss, distributed dealings ledgers accessible from an outsizedinformation network has received important attention recently as a technology with the potential to disruptand transform virtually every aspect of global business. To cite just a few examples, within the past two years major financial firms including Goldman Sachs, BNY Mellon, UBS, and the New York City Depository Trust and Clearing Corporation have announced plans to move trillions of dollars to blockchain in 2018. Blockchain applications have also been implemented in the global shipping industry to track import/export requirements, for tracking manufacturing raw materials and components in the airline industry, for tracking royalties in digital entertainment systems, for guaranteeing the safety of food chains from farm to table, and for disrupting electric utility companies using solar panels. Virtually every market vertical has begun to explore or implement blockchain as cornerstones of their next generation technology roadmaps. Many of those new services are hosted in cloud computing environments; the pinnacle of economic Services Business Development for Amazon internet Services has commented "distributed ledger technology is at the forefront of any discussion associated with innovation". This widespread interest in blockchain distributed ledgers is accompanied by growing concerns regarding cyber security. Both the number and severity of cyber security incidents have grown dramatically in the past few years. Many of these attacks can be attributed, at least in part, to a lack of rigorous authentication and identity management, protection against insider threats, and lack of rigorous compliance auditing. For example, in May of 2016 an attack on the global financial messaging network known as SWIFT resulted in over $80 million in losses to banks in Bangladesh, the Philippines, Sri Lanka, Vietnam, and elsewhere. A lack of authentication contributes to distributed denial of service attacks (DDoS), such as when the Mirai botnet unleashed a record-setting 1.2 Terabit/second attack against

the service provider Dyn disrupting their DNS service and impacting countless users on Twitter, Amazon, Spotify, Netflix, Tumblr, and Reddit.When the Mirai ASCII text file was free shortly thenceforth, variants reportedly disrupted banks and telecom carriers in Russia, Germany, and the United Kingdom.

These examples are part of an unfortunate rising trend in cyberattacks, which motivate an urgent need for improved defensive capabilities. A elementary issue with current blockchain service proposals could be a lack of authentication, identity management, and no repudiation, along with the associated resistance to DDoS attacks. In this paper, we present results from our experimental cyber security cloud test bed which implements a novel approach to user identity management in blockchain services.

We implement identity-based end-to-end security that extends from the blockchain consumer to the server-side application and material. We conjointly demonstrate identity-based network segmentation and traffic separation, which enables multiple users to securely share the same blockchain infrastructure, reduces the risk of DDoS attacks, and enables automated regulatory compliance audits. Our answer is predicated on a mixture of BlackRidge initial Packet Authentication™ and BlackRidge Transport Access management (TAC) technologies, enforced victimisation software system endpoints and entryway appliances from BlackRidge Technology.

Experimental results will be provided for a sample resource 474 trading application using IBM's version of the open source Hyperledger framework. Our approach can easily be generalized to protect many different types of commercial applications.

J. W. BOS, J. A. HALDERMAN, N. HENINGER, J. MOORE, M. NAEHRIG, AND E. WUSTROW, "ELLIPTIC CURVE CRYPTOGRAPHY IN PRACTICE," IN FINANCIAL CRYPTOGRAPHY AND DATA SECURITY. SPRINGER, 2014, PP. 157–175.

In this paper, we perform a review of elliptic curve cryptography (ECC), as it is used in practice today, in order to reveal unique mistakes and vulnerabilities that arise in implementations of ECC. We study four popular protocols that make use of this type of public-key cryptography: Bitcoin, secure shell (SSH), transport layer security (TLS), andthe Austrian e-ID card. We are pleased to observe that about 1 in 10 systems support ECC across the TLS and SSH protocols. However, we _nd that despite the high stakes of money, access and resources protected by ECC, implementations su_er from vulnerabilities similar to those that plague previous cryptographic systems.

P. KOSHY, D. KOSHY, AND P. MCDANIEL, AN ANALYSIS OF ANONYMITY IN BITCOIN USING P2P NETWORK TRAFFIC. SPRINGER, 2014.

Over the last 4 years, Bitcoin, a decentralized P2P crypto- currency, has gained widespread attention. The ability to create pseudo-anonymous financial transactions using bitcoins has made the currency attractive to users who value their privacy. Although previous work has analyzed the degree of anonymity Bitcoin overs using clustering and own analysis, none have demonstrated the ability to map Bitcoin ad-dresses directly to IP data. We propose a novel approach to creating and evaluating such mappings solely using real-time transaction traffic collected over 5 months. We developed heuristics for identifying ownership relationships between Bitcoin addresses and IP addresses. We discuss the circumstances under which these relationships become apparent and demonstrate how nearly 1,000 Bitcoin addresses can be mapped to their likely owner IPs by leveraging anomalous relaying behavior.

E. ANDROULAKI, G. O. KARAME, M. ROESCHLIN, T. SCHERER, AND S. CAPKUN, "EVALUATING USER PRIVACY

IN BITCOIN," IN FINANCIAL CRYPTOGRAPHY AND DATA SECURITY. SPRINGER, 2013, PP. 34–51.

Bitcoin is quickly emerging as a popular digital payment system. However, in spite of its reliance on pseudonyms, Bitcoin raises a number of privacy concerns due to the fact that all of the transactions that take place are publicly announced in the system. In this paper, we investigate the privacy provisions in Bitcoin when it is used as a primary currency to support the daily transactions of individuals in a university setting. More specifically, we evaluate the privacy that is provided by Bitcoin (i) by analyzing the genuine Bitcoin system and (ii) through a simulator that faithfully mimics the use of Bitcoin within a university. In this setting, our results show that the profiles of almost 40% of the users can be, to a large extent, recovered even when users adopt privacy measures recommended by Bitcoin. To the best of our knowledge, this is the first work that comprehensively analyzes, and evaluates the privacy implications of Bitcoin.

BIEHL, B. MEYER, AND V. M¨ ULLER, "DIFFERENTIAL FAULT ATTACKS ON ELLIPTIC CURVE CRYPTOSYSTEMS," IN ADVANCES IN CRYPTOLOGY- CRYPTO 2000. SPRINGER, 2000, PP. 131–146.

In this paper we extend the ideas for deferential fault at- tacks on the RSA cryptosystem (see [4]) to schemes using elliptic curves. We present three deferent types of attacks that can be used to derive information about the secret key if bit errors can be inserted into the elliptic curve computations in a tamper-proof device. The electiveness of the attacks was proven in a software simulation of the described ideas.

EXISTING SYSTEM:

Databases applications consensus is enormous and it promises to disrupt the current ecosystem that tends to the monopoly.Companies like eBay, Facebook and Uber are very valuable because they benefit tremendously from the network effects that come back from keeping all user info centralised privately silos and the way they act as middle men taking a cut of all the transactions. Decentralised protocols on prime of the blockchain have the potential to undo each single a part of the stacks that build these services valuable to customers and investors. They can try this by, as an example, making common, suburbanised information sets to that anyone will plug into, and sanctioning peer-to-peer transactions powered by bitcoin and different cryptocurrencies.

DISADVANTAGES:

- No empty blocks are Placed
- Easy to identify the travelling path of data

PROPOSED SYSTEM:

Smart contracts ar contracts whose terms ar recorded in a very machine-oriented language rather than legal language. Smart contracts is mechanically dead by a computer system, like an appropriate distributed ledger system. The potential advantages of sensible contracts embrace low getting, social control, and compliance costs; consequently it becomes economically viable to create contracts over varied low-value transactions. So the question behind Blockchain is why rely on a central authority once 2 (or more) parties will agree between themselves, and after they will bake the terms and implications of their agreement programmatically and conditionally.

ADVANTAGES:

- Additionally empty blocks are added
- Encrypt key used to data transaction as additional security
- Unauthorised person could not able to access.

MODULE DESCRIPTION

- Key Generation:
- Key generation using Block chain:
- Tag Generation:
- Data Verification:

Available@ www.ijrse.org Mail: info@ijrse.org ISSN: 2212-4012

- Dynamic Data & User Audit:
- Index hash Table:

Key Generation:

The owner generates a public/secret key pair by himself or the system manager, and then sends his public key pk to TPA. Note that TPA cannot obtain the client's secret key sk; secondly, the owner chooses the random secret.The key feels like, should do the right thing with their cloud strategy and make sure that they ask the right questions to their cloud service providers. It isn't really about whether or not the service has encryption or not.

Key generation using Block chain:

Each block contains a cryptographic hash of the previous block,a timestamp, and transaction data A cryptographic hash function is a special class of hash function that has certain properties which make it suitable for use in cryptography. It is a mathematical algorithmic program that maps knowledge of discretional size to a small amount string of a set size (a hash) and is meant to be a unidirectional operate By design, a blockchain is immune to modification of the info.

Tag Generation:

The client (data owner) uses the secret key sk to pre-process a file, which consists of a collection of n blocks, generates a set of public verification parameters and index-hash table that are stored in TPA, and transmits the file and some verification tags to CSP.Tags generated by DOs and the leakage of the user's secret key

Data Verification:
Authority issues a "Random Sampling" challenge to audit the integrity and availability of outsourced data in terms of the verification information stored in TPA it is crucial to develop a more economical and secure mechanism for dynamic audit services, in which a potential adversary's advantage through dynamic data operations

Dynamic Data & User Audit:
An authorized application, that holds knowledge owner's secret key, will manipulate the outsourced knowledge and update the associated index hash table keep in storage. The privacy and the checking algorithm ensure that the storage server cannot cheat the authorized applications and forge the valid audit records.

Index hash Table:

To support dynamic data operations, we introduce a simple IHT to record the changes of file blocks, as well as generate the hash value of each block in the verification process. The structure of our IHT is similar to that of file Block allocation table in file systems. Generally, the IHT consists of serial number, block number, version number, and random integer Note that we must assure all records in the IHT differ from one another to prevent the forgery of data blocks and tags. In addition to recording data changes, each record in the table is used to generate a unique hash value, which in turn is used for the construction of a signature tag by the secret key

SYSTEM ARCHITECTURE

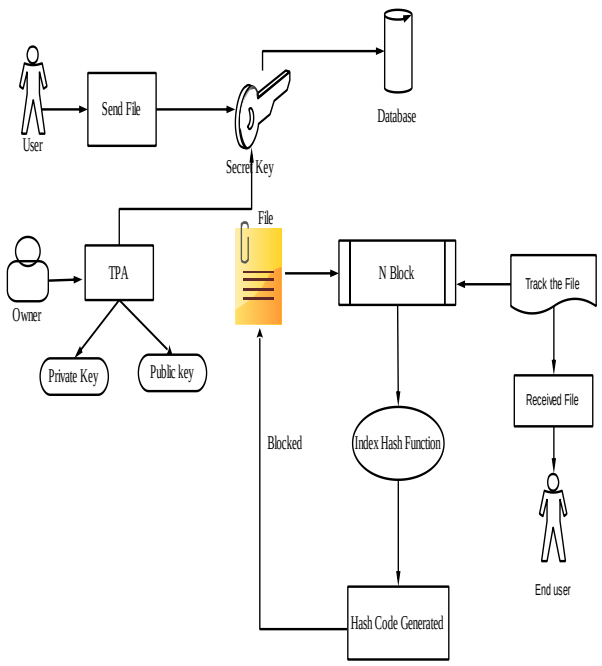

Figure 1: Architecture

CONCLUSION

A construction of dynamic audit services for un-trusted and outsourced storages. We conjointly given AN economical methodology for periodic sampling audit to boost the performance of TPAs and storage service suppliers. This project developed in Windows Mysql Cloud, mainly this cloud improves the security and performance.

REFERENCES

[1] A. Nordrum, "Wall Street firms to move trillions to blockchain in 2018", IEEE Spectrum, October 2017, https://spectrum.ieee.org/telecom/internet/wall-street-firms-to-movetrillions- to-blockchains-in-2018 (last accessed November 20, 2017)

[2] K. Lewis, "Blockchain: four use cases transforming business", IBM Internet of Things blog, May 2017 https://www.ibm.com/blogs/internetof- things/iot-blockchain-use-cases/ (last accessed November 20, 2017)

[3] K. Lotay and C. DeCusatis, "Using blockchain technology to digitize supply chain systems", Proc. National Conference on Undergraduate Research, Atlanta, GA, Nov. 3-5, 2017

[4] M. Peck, "Blockchains: how they work", IEEE Spectrum, October 2017, https://spectrum.ieee.org/computing/networks/blockchains-how-theywork- and-why-theyll-change-the-world (last accessed November 20, 2017)

[5] M. Peck and D. Wagman, "Blockchains allow rooftop solar energy trading", IEEE Spectrum, October 2017 https://spectrum.ieee.org/computing/networks/blockchains-will-allowrooftop- solar-energy-trading-for-fun-and-profit (last accessed November 20, 2017)

[6] A.Flores & K. Gannon, "BlockChain on AWS: Disrupting the Norm", paper GPSD301, AWS Re:Invent 2016 (November 29, 2016) https://www.slideshare.net/AmazonWebServices/aws-reinvent-2016- blockchain-on-aws-disrupting-the-norm-gpst301 (last accessed September 20, 2017)

[7] Cisco Institution, "Cisco 2017 annual cybersecurity report," Cisco, Tech. Rep., 2017.

[8] Mikko Hypponen. and Tomi Tuominen., "F-Secure 2017 State of Cybersecurity report," F-Secure, Tech. Rep., 2017.

[9] S. Nakamoto, "Bitcoin: a peer to peer electronic cash system", Oct. 31, 2008 http://nakamotoinstitute.org/bitcoin/. http://bitcoin.org/bitcoin.pdf. https: //github.com/saivann/bitcoinwhitepaper. (last accessed Sept. 20, 2017)

[10] R. Miller, "IBM unveils HyperLedger project", March 19, 2017, https://techcrunch.com/2017/03/19/ibm-unveils-blockchain-as-a-servicebased- on-open-source-hyperledger-fabric-technology/ (last accessed September 20, 2017)

[11] M. Russinovich, "The Coco framework for enterprise blockchain networks", August 10, 2017 https://azure.microsoft.com/enus/ blog/announcing-microsoft-s-coco-framework-for-enterpriseblockchain- networks/ (last accessed November 20, 2017)

[12] T. Khurana, "Cisco Internet of Things blockchain protocol initiative", August 1, 2017, https://blogs.cisco.com/tag/blockchain-iot-protocolinitiative (last accessed November 20, 2017) [13] Enterprise Etherium Alliance press release, July 18, 2017 https://entethalliance.org/enterprise-ethereum-alliance-becomes-worldslargest- open-source-blockchain-initiative/ (last accessed November 20, 2017)

[14] J. Lang, "Three uses for blockchain in banking", October 23, 2017, https://www.ibm.com/blogs/blockchain/2017/10/three-uses-forblockchain- in-banking/ (last accessed November 20, 2017)

[15] IBM Press Release, BlockChain at Interconnect 2017 conference, March 21, 2017 (last accessed September 26, 2017)

BIOGRAPHICAL NOTES

	Mrs.Kayalvizhi.R - Received M.C.A.,M.Phil.,.She has 12 Years of Teaching Experience.She is Guided 7 Students in M.Phil.,She had Presented 3 Papers Presentations and She Presented 10 Papers in National Conference.She is Currently Working as Assistant Professor in Department of Computer Applications in Dhanalakshmi Srinivasan College of Arts & Science for Women(Autonomous),Perambalur,TamilNadu,India.
	Ms..Bhuvaneswari.G.,PG Scholar,[Department of Computer Applicatons],pursuing MCA in Dhanalakshmi Srinivasan College of Arts & Science for Women(Autonomous), ,Perambalur-621212,TamilNadu,(India).