Ph.D. Progress Report

December- 2018
Ravi Kanth Kotha (717145)

1 Introduction:

Present days, information and communication technology has been an integral part of business processes. It provides tools and functions on which almost all companies thourghtout the world runs. And the way in which the customers interact with business services is also evolving rapidly. With the rising consumer expectations, combined with increased competition and rapid technological advancements has led to an environment where the capabilities of modern technologies has to be leveraged to provide availability, scalability, privacy, end-to-end security and asynchronous business processes.

2 Literature Survey:

A typical business process today involves processing and exchange of information among multiple stakeholders in a distributed environment. In the current centralized IT systems information is processed and shared from one party to another using multiple hops. In such a scenario, it is important that all the participants are accessing and acting on the same information, and have the same understanding about the state (success / failure / current status) of the transaction. This requirement is referred to as end-to-end security, which is missing in the current systems. Keeping security as the core area of interest, currenlty we are exploring the following topics.

- Distributed Systems
- Blockchain Technology
- End-to-End Security

2.1 Distributed Systems

A distributed system is defined as a system whose components are located on different networked (geographically) computers, which then communicate and coordinate their actions by passing messages to one another in order to achieve a common goal. A rich theory is available on distributed systems developed for over the past four decades. Distributed systems are very complex to design and implement and require several properties such as consensus algorithms (PAXOS, PBFT) [15] [14] [13] [6] [5], fault tolerance [1] [9] [17] and communication models [3] [7]. A practical consistent fault tolerant distributed system can be achieved using a technique called state machine replication (SMR) [4] [20], which is a general method of implementing a software service by replicating servers and coordinating client interactions with server replicas.

2.2 Blockchain Technology

The first work on a cryptographically secured chain of blocks was described in 1991 by **Stuart Haber and W. Scott Stornetta** [8]. The idea is to implement a system where document timestamps (logical) could not be tampered. In 1992, Bayer, Haber and Stornetta incorporated Merkle trees [2] to the above implementation, which improved its efficiency by allowing several document certificates to be collected into one block.

The first Blockchain was conceptualized by Satoshi Nakamoto in 2008 [16]. Nakamoto improved the design using a Hashcash-like method to add blocks to the chain without requiring them to be signed by a trusted third party. The design was implemented as a core component of the cryptocurrency called bitcoin. Bitcoin then came into existence to be used as an off-line digital currency. The term Blockchain 2.0, introduced by Ethereum refers to a new kind of application of the distributed Blockchain database. Blockchain 2.0 is described as a second-generation programmable Blockchain coming with a programming language that allows users to write more sophisticated smart contracts which creates invoices that pay themselves when a shipment arrives.

Bitcoin and Ethereum Blockchain technologies are permissionless Blockchains [21] where all the data will be accessible to all the participants. This makes these Blockchain technologies not suitable for business use cases. And hence permissioned Blockchain technologies are introduced to address the organizational use cases. Some of the existing permissioned Blockchain technology platforms are Hyperledge Fabric, Corda, Multichain and Quorum Systems. On a detailed study of these platforms it is observed that there are some inevitable trade-offs in each platform. A comparative study of these permissioned platforms have been developed and accepted in IWBT-2018. A quick look on the summary of the comparitive study reveals that Hyperledger Fabric is best suitable for applications that demand high business continuity and end-to-end security, and can tolerate slight loss of privacy restricted to within a channel. Corda is best suited for applications that demand high privacy and throughput. Business continuity and end-to-end security are adversely effected due to the design choice of Corda.

2.3 End-to-End Security

Security at data layer has been the interest of research for a long time. Currently, there are advanced tools available to secure data at rest. But securing data in transit or in the state of processing is as important as the securing data being stored. This data can be secured using Information Flow Control (IFC) systems where the research in this area has also been in much of interest. A combination of both research areas can provide an end-to-end security system which secures data that is being stored as well as data under processing.

Lattice-based access control models (LBAC) initiated by Bell-LaPadula (BLP) / Biba models, and consolidated by Denning have played a vital role in building secure systems via Information Flow Control. IFC systems typically label data and track labels, while allowing users to exercise appropriate access privileges. Although there has been a tremendous effort being done on information flow control systems for three decades, practical tools are not available to evaluate the security protocols in IFC systems.

Recently, Readers-Writers Flow Model (RWFM) [11] a new IFC model was introduced based on the Denning model of information flow in a system. RWFM establishes a strong relation between syntactic and semantic labels of an object and a subject within a system. RWFM provides an application-independent concrete generative labeling, which is sound and complete. RWFM label provide a formalization for privacy policies, provides an algorithm for checking policy conformance [12]. The applicability of RWFM has been proved in a variety of contexts to: verify the design of security protocols[10], analyze the security of the EMV protocol to explicitly capture the intentions of the protocol designer[18], and build a runtime monitor for the Android environment[19].

3 Future Work Planned:

1. Understood the pitfalls in the area of distributed systems where there is need to tweak or modify the classic distributed system algorithms(Paxos, PBFT) to accommodate the current business requirements.

2. Distributed computing platform using Blockchain: challenge is to design application layer in such a way as to preserve the end-to-end security in a business process.

4 Conclusion:

A variety of business services offered today involve interactions between multiple stakeholders. To make these interactions secure it is not sufficient to have just data being secured but requires an end-to-end secure application. The objective of this thesis is to design and develop an end-to-end secure distributed system using blockchain

References

[1] Michael Abd-El-Malek, Gregory R Ganger, Garth R Goodson, Michael K Reiter, and Jay J Wylie. Fault-scalable byzantine fault-tolerant services. *ACM SIGOPS Operating Systems Review*, 39(5):59–74, 2005.

[2] Dave Bayer, Stuart Haber, and W Scott Stornetta. Improving the efficiency and reliability of digital time-stamping. In *Sequences II*, pages 329–334. Springer, 1993.

[3] Michael Ben-Or. Another advantage of free choice (extended abstract): Completely asynchronous agreement protocols. In *Proceedings of the second annual ACM symposium on Principles of distributed computing*, pages 27–30. ACM, 1983.

[4] Alysson Neves Bessani and Eduardo Alchieri. A guided tour on the theory and practice of state machine replication. In *Tutorial at the 32nd Brazilian symposium on computer networks and distributed systems*, 2014.

[5] Miguel Castro and Barbara Liskov. Practical byzantine fault tolerance. In *Proceedings of the Third USENIX Symposium on Operating Systems Design and Implementation (OSDI), New Orleans, Louisiana, USA, February 22-25, 1999*, pages 173–186, 1999.

[6] Miguel Castro and Barbara Liskov. Practical byzantine fault tolerance and proactive recovery. *ACM Transactions on Computer Systems (TOCS)*, 20(4):398–461, 2002.

[7] Michael J Fischer, Nancy A Lynch, and Michael S Paterson. Impossibility of distributed consensus with one faulty process. Technical report, MASSACHUSETTS INST OF TECH CAMBRIDGE LAB FOR COMPUTER SCIENCE, 1982.

[8] Stuart Haber and W Scott Stornetta. How to time-stamp a digital document. In *Conference on the Theory and Application of Cryptography*, pages 437–455. Springer, 1990.

[9] Ramakrishna Kotla, Lorenzo Alvisi, Mike Dahlin, Allen Clement, and Edmund Wong. Zyzzyva: speculative byzantine fault tolerance. *ACM SIGOPS Operating Systems Review*, 41(6):45–58, 2007.

[10] N. V. Narendra Kumar and R. K. Shyamasundar. Analyzing protocol security through information-flow control. In *Distributed Computing and Internet Technology - 13th International Conference, ICDCIT 2017, Bhubaneswar, India, January 13-16, 2017, Proceedings*, pages 159–171, 2017.

[11] N. V. Narendra Kumar and R. K. Shyamasundar. A complete generative label model for lattice-based access control models. In *Software Engineering and Formal Methods - 15th International Conference, SEFM 2017, Trento, Italy, September 4-8, 2017, Proceedings*, pages 35–53, 2017.

[12] N. V. Narendra Kumar and R. K. Shyamasundar. Dynamic labelling to enforce conformance of cross domain security/privacy policies. In *Distributed Computing and Internet Technology - 13th International Conference, ICDCIT 2017, Bhubaneswar, India, January 13-16, 2017, Proceedings*, pages 183–195, 2017.

[13] Leslie Lamport. Time, clocks, and the ordering of events in a distributed system. *Communications of the ACM*, 21(7):558–565, 1978.

[14] Leslie Lamport. The part-time parliament. *ACM Transactions on Computer Systems (TOCS)*, 16(2):133–169, 1998.

[15] Leslie Lamport, Robert Shostak, and Marshall Pease. The byzantine generals problem. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, 4(3):382–401, 1982.

[16] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system, http://bitcoin.org/bitcoin.pdf.

[17] Brian M Oki and Barbara H Liskov. Viewstamped replication: A new primary copy method to support highly-available distributed systems. In *Proceedings of the seventh annual ACM Symposium on Principles of distributed computing*, pages 8–17. ACM, 1988.

[18] Khedkar Shrikrishna, N. V. Narendra Kumar, and R. K. Shyamasundar. Security analysis of EMV protocol and approaches for strengthening it. In *Distributed Computing and Internet Technology - 14th International Conference, ICDCIT 2018, Bhubaneswar, India, January 11-13, 2018, Proceedings*, pages 69–85, 2018.

[19] R. K. Shyamasundar, N. V. Narendra Kumar, and Priyanka Teltumde. Realizing software vault on android through information-flow control. In *2017 IEEE Symposium on Computers and Communications, ISCC 2017, Heraklion, Greece, July 3-6, 2017*, pages 1007–1014, 2017.

[20] João Sousa, Eduardo Alchieri, and Alysson Bessani. State machine replication for the masses with bft-smart. 2013.

[21] Roger Wattenhofer. *The science of the blockchain.* Inverted Forest Publishing, Erscheinungsort nicht ermittelbarUSA, 2016.