SHAHJALAL UNIVERSITY OF SCIENCE AND TECHNOLOGY

THESIS PROPOSAL

SELF SOVEREIGN IDENTITY MANAGEMENT SYSTEM

by

Md. Mesbah Uddin Waheed(2016331042)
Tapu Das(2016331106)

Supervised by
Md Sadek Ferdous
Assistant Professor, Department of CSE, SUST

Department of Computer Science and Engineering
Shahjalal University of Science and Technology
Date: 09-03-2020

TABLE OF CONTENTS

1. INTRODUCTION

1.1 Motivation

When services and resources are available through a computer network, it is important to know who the users are and to control what services they are authorised to use. For an example, we need to sign up or login in different kinds of websites. To access these websites, we need passwords. In many websites they have their own criteria for giving password. We need to memorise these passwords for accessing various kinds of websites. It is tough to memorise all the passwords. In this state of affairs, identity management helps users with credentials and authenticating users. It also helps users control their access to services and resources based on their identifiers and credentials. The proposed system allows users to have complete control over their own data and to improve the privacy of the user while accessing online services. For security issues , here we introduce Blockchain technology with an identity management system. Blockchain exhibits several properties which coincides with some desirable properties of a self-sovereign identity. By integrating Blockchain technology with the Self-Sovereign identity management system, we can propose a solution that is designed to be cost effective and scalable from the user's perspective.

1.2 Problem Statement

In this enormous pool of online services identity has become a major criteria for authenticating users.Through interaction with other users, an established online identity acquires a reputation, which enables other users to decide whether the identity is worthy of trust. Online identities are associated with users through authentication, which typically requires registration and logging in[5].The thing is users end up with a number of different identities for different websites.The management of these identities have become increasingly difficult for users across multiple service providers.Furthermore, users have less control over their data and less knowledge how their data is being used.For example, when we use google services we don't know for sure that how google is storing or using our data.In this situation, users credential is at risk. This is because of this reason, we are trying to come up with a solution

with emerging technology blockchain, 'A Distributed System' integrated with a self-sovereign identity management system.

1.3 Proposed Solution

Our proposed solutions that are designed to be cost effective and scalable from the user's perspective. Self-sovereign identity systems use blockchains – distributed ledgers – so that decentralized identifiers can be looked up without involving a central directory. Blockchains don't solve the identity problem by themselves, but they do provide a missing link that allows things we've known about cryptography for decades to suddenly be used. That allows people to prove things about themselves using decentralized, verifiable credentials just as they do offline.Currently there are several identity management system have been introduced and they are workable.But as new systems are being introduced a user have to maintain different service provider because of different providers maintain different identity management system.Most of the identity model has limitation regarding the privacy issue of the users. Our thesis investigates the way to overcome this crucial situation introducing blockchain with a self-sovereign identity model that allows users to have complete control over their data without the interference of the authorities.

2. PRELIMINARY LITERATURE REVIEW

2.1 Self-Sovereign Identity

The hypothesis of Self-Sovereign Identity has appeared with the promise to acolyte a new era in the landscape of Identity where the user and only user, is to have full prestige over their identity data with strong support for a user-controlled data management facility.
A person's digital essence is now individualistic of any organization: no-one can take their identity away. To be self-sovereign, an identity system must have certain key features:

- Persistent
- Peer-based
- Privacy protecting
- Portable

There are so many related works about identity management. We studied some papers about identity management. We studied some works and acquired some knowledge about it. We have got interest in some works. Like, one work is "User centric identity management" [1]. In this paper, the proposed solutions that are formulated to be cost-effective and scalable from the users' perspective, while at the same time being coherent with traditional identity management systems. They characterized user-centric approaches to user identity management and to SP identity management respectively. It is natural to associate these two aspects of identity management in order to provide a seamless user-centric system for two-way authentication. System supported identity management on the user side, resulting in improved usability."In Search of Self-Sovereign Identity Leveraging Blockchain Technology" [3] which we are interested in so much. There are a few works in the literature which explore different aspects of self-sovereign identity. Unfortunately, the existing works are not methodological and extensive at all. Moreover, there exist different conceptions of what the term self-sovereign identity means. This paper aims to achieve this goal by providing the first-ever normal and adamant treatment of the concept of self-sovereign identity using a mathematical model. This paper examines the properties that a

self-sovereign identity should have and explores the impact of self-sovereign identity. It is an interesting work and we are interested to extend this topic.

2.2 Identity Management Models

Identity has become a crucial factor in the world of online services. For different websites, users have to sign up with different credentials which are actually a hassle to maintain. There is also security risk because nowadays these public websites can't be trusted. What are they doing with users credentials, no one knows. The security risks are mainly due to Intruders, viruses, worms, Trojans which have their own impact on the data systems. Identity Management systems encompass various technologies from the IT world, such as isolated user identity model, federated user identity model, common user identity model, Single-Sign-On, user-centric identity model, etc. Let's have a look at these traditional identity models.

2.2.1 Isolated User Identity Model [1]:

The most standard identity management model is to let service suppliers act as each written document suppliers and symbol suppliers to their purchasers. They management the namespace for a particular service domain and portion identifiers to users. A user gets separate distinctive identifiers from every service/identifier supplier he transacts with. additionally, every user can have separate credentials, like passwords related to each of their identifiers. This model, which can be called isolated user identity management, is illustrated in figure (Fig 2-1).

2.2.2 Federated User Identity Model [1]:

Identity federation links a user's identity diagonally multiple security domains, every supporting its own identity management system. once 2 domains square measure federates, the user will testimony to 1 domain and so penetration resources within the substitute domain while not having to perform an isolate login method. Identity federation offers economic blessings, further as an avail, to enterprises and their network subscribers. as an example, multiple firms will share one application, leading to cost-savings and consolidation of resources.This model, which can be called federated user identity management, is illustrated in figure (Fig 2-2).

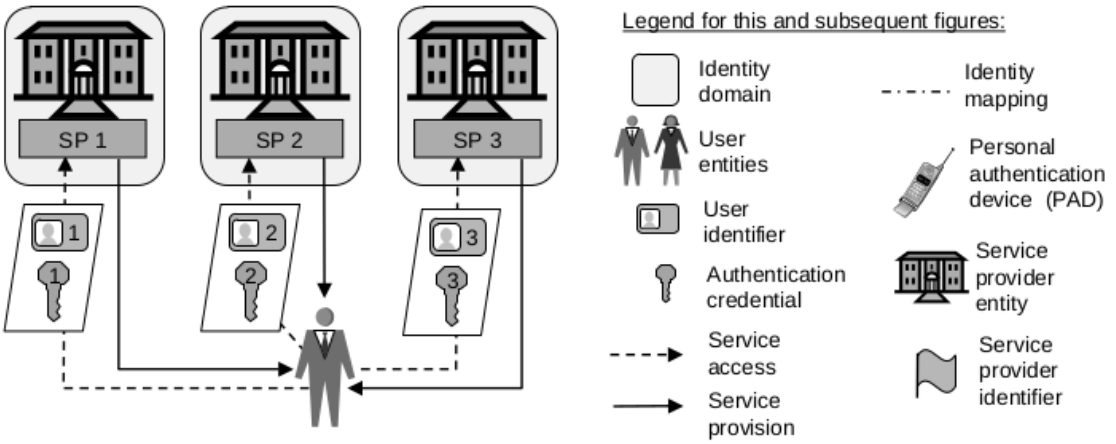

Figure 2-1: Isolated User Identity Model [1]

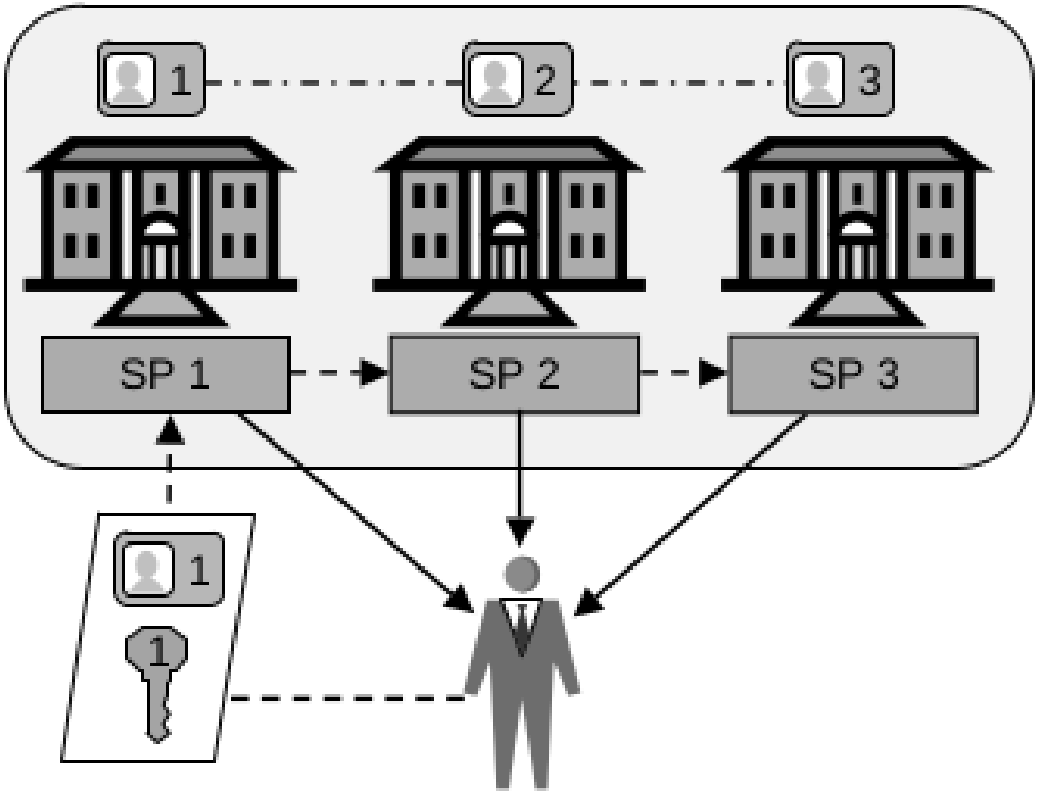

Figure 2-2: Federated User Identity Model [1]

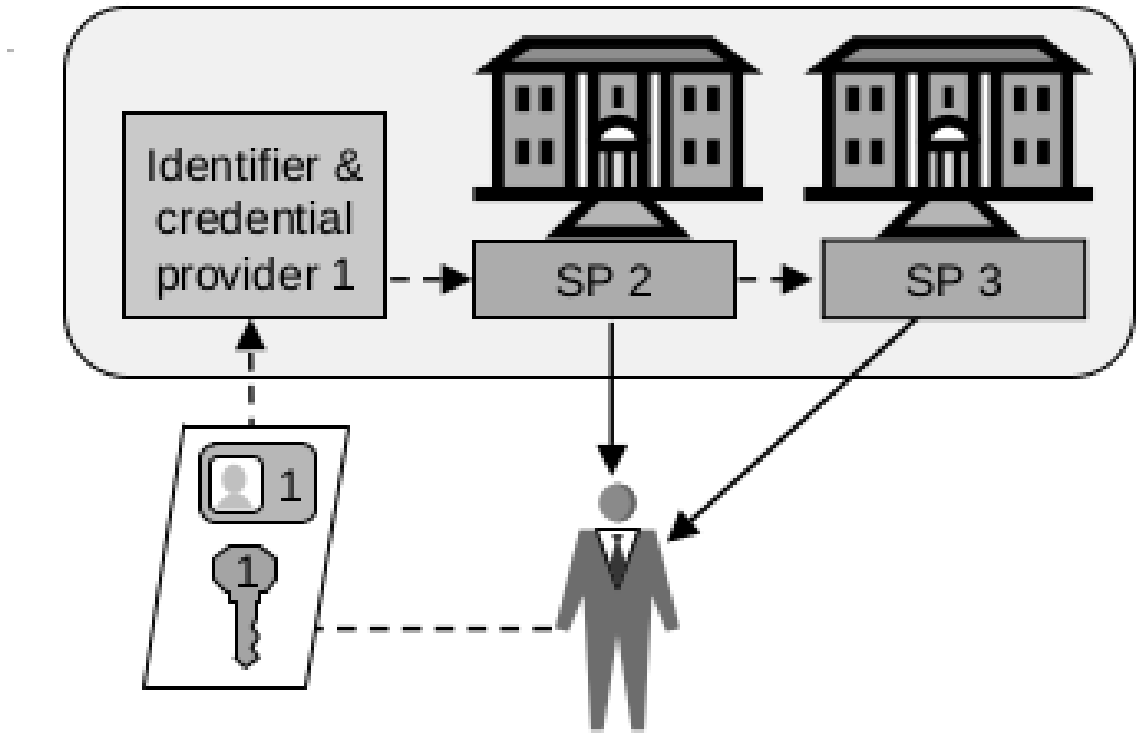

Figure 2-3: Single Sign-on Model [1]

2.2.3 Single Sign-on Identity Model [1]:

Single sign-on (SSO) is a service that authorizes a user to log into one application or network domain, then be logged in mechanically to different hooked up applications or domains. The user so solely desires one set of identity-verifying credentials (e.g. username/password) to access multiple services and applications.This model, which can be called Single Sign-on identity management, is illustrated in figure (Fig 2-3).

3. RESEARCH METHODOLOGY

As the user-base increased, service providers realized the importance of the management of user identities.Therefore identity management systems (IMS) were introduced.Different identity management systems based on different identity models are described in the previous section in this proposal.Users of these models use online services using respective protocol so that online services can be proper monitored. Currently several systems do exist as mentioned above.People working on these identity management systems are trying to make their system better but it's manageable for limited users. In this immense pool of online services it is always hard to manage huge amounts of users. Also, there lies the problem of security risk.Existing identity models does not handle user privacy efficiently which can affect the privacy of the user.

In recent times, due to the advancement of blockchain technology, the concept of self-sovereign identity is introduced. It has an influential effect on how users interact with each other and users privacy. While some experts might dispute this claim,blockchain has already demonstrated its potential,which with proper regulation, have the potential to become the new global identity management system.The ability to link blockchain-based applications to smart contracts has the potential to massively improve on existing systems and in turn, save companies huge amount of work and money.So we proposed a solution to these crucial problems integrating blockchain and self-sovereign identity management system[3].Being a distributed technology, it secures the privacy of users.Blockchain ensures the immutability of the data in the ledger. Combining with a self-sovereign identity system, blockchain can easily solve existing problems for managing identities.To access the majority of the services users have to provide their credentials.To access different services, users end up having scattered identities which are difficult to manage.To control this situation, we are proposing a self-sovereign identity management system integrated to blockchain. Self-sovereign ensures the users to control their credential without intervention of the service providers.

Considering these amazing features, we planned our whole thesis into

theses steps:

- Thread Modelling
- Requirement analysis
- Architectural Design
- Protocol and Security Design
- Protocol Develop
- Implementation
- Security Analysis
- Performance Analysis

4. FINDINGS

As the world continues to evolve and become more friendly with the adoption of new technology, the need to provide an efficient and secure way to store crucial information becomes more and more prevalent to organizations of all sizes. This demand can be met by properly implementing an effective identity management system. Identity management System (IDM) is defined as "the set of business processes, information and technology for managing and using digital identities." It encompasses everything ranging from password management to single sign-on.Though existing identity models fail to ensure the security of the user data and scatterness of identity along services.Our solution proposed self-sovereign identity system integrated with blockchain technology since existing identity models does not allow user to have control over their data and have limitations that can affect the privacy of the user. Our hope is that our solution will help to make a better user-friendly identity model.we believe that our solution will have a huge effect on identity management system as we care to make a more secure, trusted and time efficient identity model.

5. RESEARCH STUDY PLAN

Typically a study plan or work schedule that includes deliverable and milestones with the help of a Gantt chart.

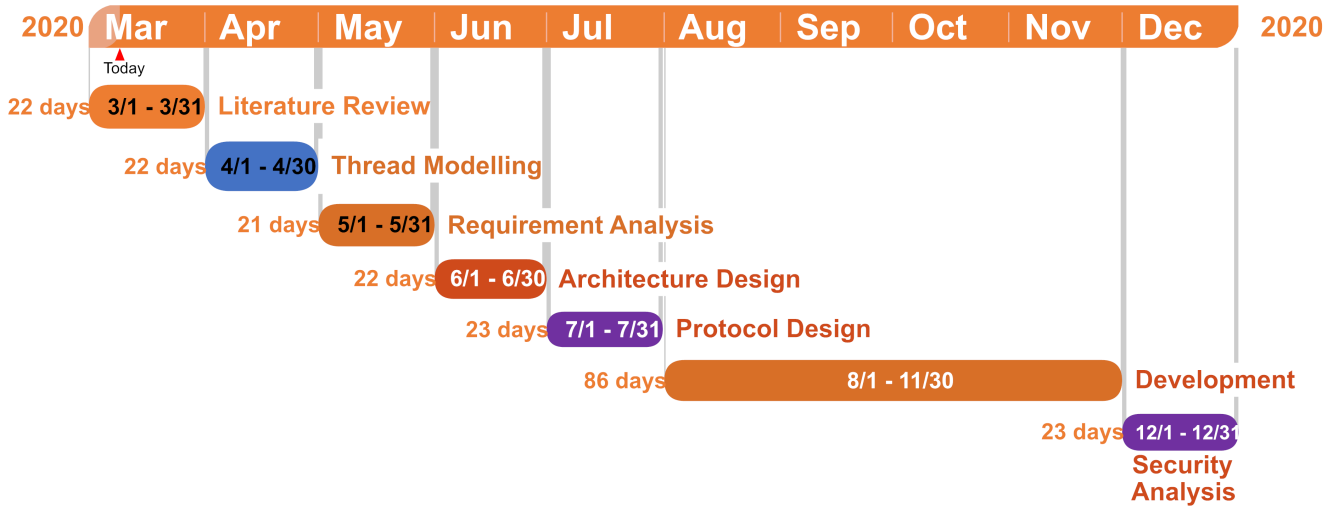

Figure 5-1: Gantt chart

6. REFERENCES

Bibliography

[1] A. Jøsang and S. Pope, "User Centric Identity Management," in Asia Pacific Information Technology Security Conference, Australia, p. 77-89, 2005.

[2] M. S. Ferdous, "User-controlled identity management systems using mobile devices," Ph.D. dissertation, School Comput. Sci., Univ. Glasgow, Glasgow, Scotland, 2015.

[3] Ferdous, Md. Sadek.& Chowdhury, Farida.& Alassafi, Madini.(2019).In Search of Self-Sovereign Identity Leveraging Blockchain Technology. IEEE Access. 7. 1-1. 10.1109/ACCESS.2019.2931173.