Distributed, Secure, Self-Sovereign Identity for IoT Devices

Samson Kahsay Gebresilassie
British Telecom Ireland Innovation Centre
School of Computing
Ulster University
Jordanstown, Northern Ireland, BT37 0QB UK
gebresilassie-s@ulster.ac.uk

Dr. Joseph Rafferty
British Telecom Ireland Innovation Centre
School of Computing
Ulster University
Jordanstown, Northern Ireland, BT37 0QB UK
j.rafferty@ulster.ac.uk

Prof. Philip Morrow
British Telecom Ireland Innovation Centre
School of Computing
Ulster University
Jordanstown, Northern Ireland, BT37 0QB UK
pj.morrow@ulster.ac.uk

Zhan Cui
British Telecom
Adastral Park
Martlesham, Ipswich, UK
zhan.cui@bt.com

Prof. Liming (Luke) Chen
British Telecom Ireland Innovation Centre
School of Computing
Ulster University
Jordanstown, Northern Ireland, BT37 0QB UK
l.chen@ulster.ac.uk

Dr. Mamun Abu-Tair
British Telecom Ireland Innovation Centre
School of Computing
Ulster University
Jordanstown, Northern Ireland, BT37 0QB UK
m.abu-tair@ulster.ac.uk

***Abstract*—The growth of Internet use due to the emergence of new paradigms including social media and the Internet of Things (IoT) has presented several challenges. Within the IoT paradigm, there are several domain-specific challenges, among which security is crucial. Billions of devices in the IoT ecosystem have the responsibility of generating, processing, and analyzing large volumes of data. This data may connect with organizations, services, billions of people and other devices. This high level of interconnectivity creates a complex, heterogeneous, network which is challenging to adequately secure. IoT devices are smart, diverse, portable, interoperable, often autonomous and deployed in distributed topology.**

Properly managing the identities of these IoT devices plays a critical role in achieving the security of the overall IoT ecosystem. Notably, existing identity management systems fail to satisfy the requirements of identity management for IoT devices. We present a novel solution for IoT devices identity management based on self-sovereign identity and underpinned by proven security offered by distributed ledger technology. This novel approach provides a secure, portable, decentralized, persistent, unique, interoperable, self-owned and controlled identity. A Device's identity with all its relationships in the IoT system are securely managed throughout its entire lifecycle.

Keywords*— *Digital Identity, Internet of things, self-sovereign identity, Distributed Ledger Technology, blockchain, IoT security.

I. Introduction

Due to the rapid growth of millions of online services, billions of users and devices, digital identities have become complex and difficult to manage (1). As the Internet of Things (IoT) paradigm is growing in scale and scope leading to different interactions among devices, services, and people. This is creating less secure communication and inadequate authenticity of information in the IoT ecosystem. As a result of this the IoT ecosystem became challenging to achieve security, scalability, availability, and usability.

A key pillar of security is a robust identity management systems wherein users, devices, services and organizations that interact over the Internet need to be represented by a digital identity (2). An IDentity Management System (IDMS) is a framework with a set of rules used to commission, manage and retire digital identities. Digital identities uniquely identify a subject in a given context, enabling interaction, anonymously or non-anonymously between secure subjects.

IDMS leverage a combination of many technologies but it can be grouped in to four main elements: Service Provider(SP), IDentity Provider (IDP), identity verifier and identity subject/user (3). The SP, sometimes called a relying party, is an entity that provides services to entities like end users and things. An IDP is an entity whose role is to create, manage, maintain, and maintain credentials and asserting issued credentials of subscribers (users) during authentication (4). Identity verifier has the role of checking the correctness of user's identities provided by the SP and decides its validity. A user in the general term, is the client of both SP and IDP about whom claim is assigned for. Identity holder could be a range of participants within an IoT ecosystem including; a person, an organization, an application software (service) or an IoT device.

Existing IDMSs rely on a single centralized authority which has insecure authenticity, limited scalability, represents a single point of failure, suffers from non-persistent availability of services and is susceptible to identity theft (5). Moreover, mobility of devices, their dynamic topology, diversified functionality, unstandardized protocols, and missing inherent security of IoT devices during manufacturing worsen the security challenge in the entire IoT system (6)(7). Some recent and emerging decentralized identity-based IDMSs address some IoT-related identity problems but are limited in their approach focusing on human identities, scalability and performance issues. Thus, IoT devices require a new digital identity mechanism that can overcome these challenges and provide suitable identity management requirements in the IoT system. This research investigated existing IDMSs and identifies problems and opportunities with respect to IoT device identity management requirements and then developed a novel a solution.

II. RELATED WORK

Existing IDMSs could be categorized into two domains, traditional and decentralized in operation. The traditional IDMSs are mainly dependent on a centralized IDP which performs all operations of creating, updating, managing, and deleting identities across their lifecycle. Recently developed decentralized IDMSs have deficiencies in addressing the identity requirements of IoT solutions due to scalability, performance, and storage capacity issues in addition to being primarily developed for human identities (8). However, in the IoT systems, IoT devices comprise most of the identities. Thus, this section analyzes contemporary traditional and decentralized model IDMSs and identifies deficiencies which may be addressed.

A. Traditional Identity Management Systems

In traditional IDMSs, the credentials of all users are stored in the IDP. and When users need access to services, they request the SPs and the IDP determine whether to grant or deny access (3). In this model identity owners have limited or even no control of their own identities and they are dependent on the consent of the IDPs/SPs for any access to services they need and changes they made. Moreover, identity owners can be denied services, and their identities can even be taken away completely (9). One main core element of the traditional IDMSs is the Public key infrastructure (PKI). PKI is a framework that consists a set of roles, policies, and procedures aiming at issuing, managing, validating and distributing certificates and public-private keys. The conventional PKI is a centralized system used as a means of secure authentication on the Internet. It issues certificates to users through Certificate Authority (CA), maintains, backups and revokes public keys. PKI may use a certificate standard, such as X.509, to manage public keys together with a trusted third party CA that verifies ownership of the public keys (11). The X.509 standard defines the certificate format and maps public keys to the identities of the key holder. The CA asserts this binding by digitally signing each certificate based on the validity of the private certificate holder. However, PKI relies on centralized trusted party CAs that defines identities by themselves. This denies control and ownership of identities to the owners and opens ways to several attacks. Traditional identity management systems may be realized through 4 general approaches as discussed in sections 1, 2, 3 and 4.

1) Isolated Model

In the isolated model, both SP and IDP roles are consolidated and provided as a single service encapsulating both roles (9). As the Internet grows with many online services and billions of IoT devices along with a large volume of identities, the isolated model is incapable of providing scalable, secure and appropriate service to users and things. Moreover, users may need to manage hundreds, or in some cases thousands, of different credentials leading to mismanaging identities, password reuse and forgetting credentials. This increases the attack surface for individuals and introduces associated risks related to theft and reuse of identity parameters, such as the issues posed by disclosure of inadequately protected password representations.

2) Centralized Identity Model

Unlike the isolated model, the centralized identity model detaches the SP from the IDP making them function as separate roles(9). In this model a single IDP stores, issues and manages all user identities from multiple SPs. The IDP of this model implements Single Sign-On (SSO) which provide access to users of multiple SPs using same credentials with a one-time login. SSO implementation on centralized model differs from federated model (3). In the centralized identity management model SSO functions within a single security domain where the IDP and multiple SPs are governed by a single policy under a single authority (12). This model is preferred over the isolated model as it reduces the number of user identities. However, it is facing many challenges such as being a single point of failure, unscalable and targets of many vulnerabilities and attacks.

3) Federated Identity Model

Federated identity model brings multiple SPs/IDPs operating in different security domains into a federation by establishing a trusted relationship built on a set of standards and technologies (13). In this model, user identity is mapped to different domains allowing authentication after an IDP and grants access to multiple services using the same login credentials within the federation (14). This provides users more accessible management over their identities as compared to centralized model. The federated operation in this model is achieved by implementing a cross-domain SSO (15). Implementation of SSO is to function in cross domain of the federation. Federated identify based solutions face a number of challenges such as misusing identity data, inflexible identity update or modification, inconsistent and faulty identity revocation mechanisms. The federated identity model is still centralized and controlled by a few IDPs. Moreover, federated identity leads to less security trust as users are forced to form a relationship with a third party that they cannot completely trust.

4) User-Centric Identity Model

As services and domains grows authentication and authorization in the federated identity model become more. The three models previously explored are designed based on SP/IDPs' perspectives while lacking full ownership and control of identities for users (16). To address these drawbacks, a user-centric identity model was proposed to improve user experience and enhance security and privacy. This approach allows users to store their identity in their own domain, facilitating control. Users can store and manage their identities from different domains in their trusted personal authentication devices such as smart cards or smartphones (17) and decide with whom identity-related information and how it should be disclosed to a SP (18). However, the user-centric identity model relies on centralized IDPs for its full functionality like the previous three models and shares some of their drawbacks.

From the analysis performed, traditional identity management models are facing many challenges and are not suitable for use within an IoT ecosystem due to vital deficiencies. The major deficiencies include reliance on a centralized architecture, susceptibility to common attacks, inability to scale to IoT requirements, lack of compliance, and operating in a non-transparent manner.

B. Decentralized Identity Model

The decentralized identity model originates and focuses on identity owner independent of any permissions from a central authority. This is an emerging identity model that Distributed Ledger Technology (DLT) in tandem with the concept of Self Sovereign Identity (SSI). DLT is analogous to a database which securely records and performs chronological transactions, in a peer-to-peer decentralized network (19). In DLT a transaction record is maintained by all the participants. On the contrary, in conventional traditional systems a transaction record is stored in a single central authority (20). In the case of IDMS, DLT eliminates the need for intermediary entities such as IDPs and SPs enabling participants hold copies of identical data updated with consensus mechanism. In addition, DLT has more basic features that solve some of the problems of IoT devices identities such as single point of failure, provable high security and privacy, identity owner consent-based information sharing, and provides portable identity.

SSI is a decentralized identity model that provides identity holders full ownership, control, and management over their identities (21). This is achieved independent of any centralized authority which can be realized by DLT. In most current developments, different enterprises use blockchain to address the challenges that their IoT systems are facing in the IDMS arena. Blockchain is the most widely used technology among the DLT types that led to many innovations beyond the financial industry. Blockchain is a decentralized peer-to-peer network unlike the traditional centralized (client-server) architecture, based on an append-only DLT. Decentralization, integrity, immutability, non-reputability, anonymity and transparency features of the blockchain can address the distributed, heterogenous, portability and security requirements of the IoT ecosystem, mainly the identity management. IDMSs that are implemented and leverage SSI principles and blockchain are examined in sections 1,2 and 3.

1)uPort

uPort (22) is based on the SSI concept implemented on the Ethereum blockchain technology. uPort aimed to provide a decentralized identity framework that works with next-generation Decentralized applications (Dapps) and traditional centralized applications such as banking and email. uPort uses Ethereum smart contracts by addressing them with unique persistent identifiers. uPort's controller module manages the digital identity and users use a recovery module to retrieve their authentication credentials from the list of delegates that the controller holds. Delegates are entities (individuals or institutions) that the identity owner chose as delegates. The Ethereum uses the concept of Proxy which serve as addresses of smart contracts representing persistent identifiers for the users. The deficiencies of uPort include insecure delegates of a user as they are available publicly on the blockchain, inability of the mobile app to store more than one identity, and unencrypted message communicated between an application and messaging server.

2)Hyperledger Indy

Hyperledger Indy is an open-source collaborative blockchain platform whose development is led by the Linux Foundation. This has been purposely designed to provide decentralized identity management and works in a cross-domain environment (23). It aims at providing private and secure identity management with full ownership and control for users over their identity and decides on sharing and disclosure based on their consent. Indy's design is mainly human identity based and does not properly address the identity of devices.

3)ADEPT

Autonomous Decentralized Peer-to-Peer Telemetry (ADEPT) uses BitTorrent for file-sharing, Ethereum as smart-contracts handling and TeleHash for peer-to-peer messaging (24). ADEPT aims in realizing device autonomy by enabling them verify transactions among themselves without the need for any central authority. As the consensus mechanism, it uses a combination of proof-of-work and proof-of-stake. IBM in partnership with Samsung is undertaking this research and only the proof of concept of ADEPT unveiled (24). ADEPT is not based on SSI and the identity management mechanism is not explicitly stated.

Although blockchain solves some of the problems of IDMSs it faces a number of challenges. The first drawback of blockchain is the scalability issue which happens as its network expands. The scalability issue is exacerbated when applied to an IoT which may contain billions of devices. Secondly, blockchain lacks performance due to transaction latencies, synchronization, and growing large amounts of data. Storage capacity is another challenge while using blockchain with resource-constrained IoT devices making them incapable of storing a large number of transactions (25).

Derived from on the analysis made on the traditional and decentralized IDMSs the following research issues are identified: i) How may the identity of the IoT devices being managed with a decentralized IDMS? ii) How to design and implement an IDMS considering the distributed nature of the IoT ecosystem? iii) How is it possible to design an IDMS that has a trust score algorithm applicable to resource-constrained IoT devices? iv) How is it possible to design a cross-platform IDMS that handles all IoT device types of different manufacturers with their portability and native features? Finally, v) With growing vulnerabilities and attacks on the IoT system, how is the identity of IoT devices secured?

A novel solution which addresses these deficiencies and research questions is presented in Section III.

III. A NOVEL, DECENTRALIZED, SELF-SOVEREIGN IDENTITY MANAGEMENT SOLUTION

Many of the existing identity management systems primarily focus on managing user identities. However, almost all online communications performed among digital actors fundamentally involve devices. Many new technologies and business operations are expanding the demands of thousands of IoT devices to serve central roles in a variety of use cases. However, they currently operate in an insecure environment consisting of various vulnerabilities due to unpatched devices, weak passwords, physical compromise, lack of proper single and multifactor authentication and lack of fundamental security features during manufacturing to mention some. This makes IoT devices themselves potentially internal threats and attack vectors. Thus, IoT devices need a secure identity management system that satisfies scalability, security, portability, and self-controlled and owned identity in a decentralized environment. Thus, the main goal of our solution is to overcome these challenges and satisfy the requirements of IDMS in IoT systems. As explained in the 'decentralized identity model' section blockchain is not a preferred solution for IoT devices, especially for resource-constrained devices, considering the scalability, performance, and storage capacity challenges that it is facing. To overcome these limitations of blockchain, a number of other new DLT modes are undergoing development. Tangle is one of these new models which is developed by IOTA as an alternative to blockchain fundamentally focusing on IoT (26).

Tangle incorporates a Directed Acyclic Graph (DAG) based DLT developed with the main goals of reducing or eliminating transaction overhead and removing block size limit treating each transaction thus enhancing transaction rates. Moreover, the Tangle protocol merges transaction maker and validator roles enabling a node capable of both making and validating transactions (27). When a node wishes to add transactions to the tangle network, it should validate the previous two transactions eliminating the block and chaining process to enhance performance and scalability (28). In addition, tangle allows parallel validation of transactions, unlike blockchains. As the number of nodes increases, the validation rate of transactions increases. Tangle has no concept of miners and allows feeless transactions. These features make it highly scalable, performant and storage efficient DLT solution compared to blockchain. Tangle is also developed to be quantum attack resistant as it uses stronger encryption algorithm called Winternitz One-Time signature scheme to generate its public addresses. As a result of these and other related important advantages for IoT system, we have chosen tangle as the underpinning DLT for this work.

This work has the following four main contributions:

i) Building a DLT-based device profiling mechanism which involves registration of IoT devices, identifier assignment, issuance and assertion of verifiable claims. ii) Design and development of a trust score algorithm suitable for IoT devices identity management. iii) Developing risk mitigation and management mechanism to identify, categorize, and manage risks that can occur on the IDMS of IoT systems and sets countermeasures. iv) Developing a trust revocation mechanism that takes actions which include revoking trust, denying privileges, revoking public keys and identifiers, and invalidating verifiable claims.

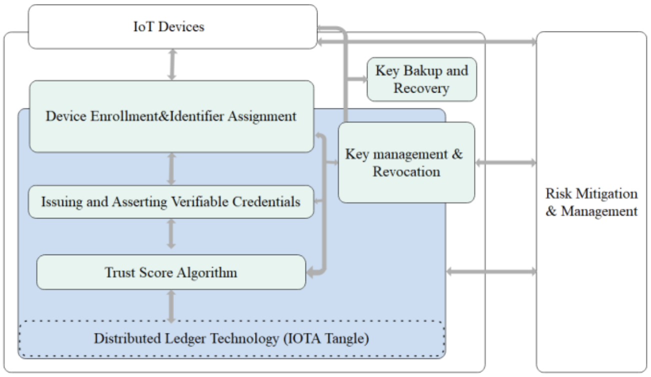
IoT Devices
Key Bakup and Recovery
Device Enrollment&Identifier Assignment
Key management & Revocation
Issuing and Asserting Verifiable Credentials
Risk Mitigation & Management
Trust Score Algorithm
Distributed Ledger Technology (IOTA Tangle)

Fig. 1. Develped architecture

Verifiable credentials (or claims) are sets of identity attributes that contains a cryptographically proof asserted by a certifying entity. Entities can share their own claims to prove self-identity without the need for sharing identity information which have greater level of privacy. The developed architecture as depicted in Figure 1, uses tangle as a foundation for the four main components of this solution: DLT based device profiling, a trust score algorithm, risk mitigation and management, and trust revocation mechanism which are briefly discussed in sub-sections A, B, C and D.

A. *DLT Based IoT Device Profiling*

Device profiling involves device enrollment, generating an identifier, generating public and private keys, and issuing and asserting verifiable claims. The identifier is generated using DLT independent of any centralized entity (registry, IDP or certificate authority). The Decentralized Identifier (DID) (29) from W3C Standard will be used to achieve decentralization, global resolvability, verifiability, secure and self-controlled features of an identifier. This enables IoT devices to fully own and manage their identifiers without relying on any centralized entity and can be used anywhere, anytime and in any environment. These identifiers are cryptographically tied to public keys and ownership is verified with the private key holding it. Following identifier mapping, the device is issued a verifiable claim which are proofs about the devices themselves. Claims or attestations for the devices can be issued by manufacturers, distributors/resellers, owners or administrators. The DLT based verifiable claims have curtail advantages in that they are scalable, allow minimum disclosure of identity information, immutable, and are truly owned by the devices themselves. The identifier and verifiable claim implemented on DLT provides a cryptographically signed tamper-proof identity for IoT devices.

B. *Trust Score Algorithm*

The TLS/SSL based web works based on the hierarchical centralized Public Key Infrastructure (PKI) to determine trusted certificates. Validating these certificates follows the chain path validation starting from the client browser to the root certificate authority. In this mechanism, the trust anchors like the browser developers and the certificate issuers are considered as trusted since their trustworthiness cannot be proofed. PKI's centralized nature leads to a single point of failure, limited scalability, and susceptibility to a number of attacks.

One such decentralized form of PKI implementation is the web of trust where users designate others as trusted by signing their public keys. As a result, a user stores his public key digitally signed by the entities that they trusted him. Others trust his certificates if they are able to verify that the certificate contains the signature of someone he or she trusts. Web of trust is preferred as it eliminates a single point of failure and builds involving multiple entities in a decentralized environment. Most IoT devices have vulnerabilities which may include weak passwords, lack of encryption, and design which does not incorporate fundamental security paradigms. Thus, adapting the web of trust for IoT devices solves many of the security problems they have through its decentralized, interoperable and secure features. As such, the trust score algorithm in this work will be built based on the basic concept of the web of trust. In addition, other parameters like minimum security requirements, reputation and compliances will be part of the trust score algorithm.

C. Risk Mitigation and Management Mechanism

Although there is a secure identity management system in place for IoT devices, there exists a risk in the IoT system like lack of fundamental security features during manufacturing. Moreover, as IoT devices involve in the collection of observational data from the physical environment, the data can originally be a victim of noise, bias, sensor drift, or manipulated by a malicious entity (30). The risk mitigation and management mechanism in this work handles these and other related risks along with the IDMS. Thus, properly authenticated devices may not always behave properly in the IoT ecosystem. A number of other risks include the inability to update firmware on time, technological advancements, growth, and nature of attacks, and other issues. Our risk mitigation and management system aims at discovering and mitigating different types of risks and ensures that these risks are reduced to an acceptable level. It also ensures that risks are properly managed and appropriate countermeasures are taken based on mitigated, identified, categorized and corresponding outcomes.

D. Trust Revocation Mechanism

A secure backup and recovery mechanism is vital in securing private keys and the overall IDMS of the IoT system. This mechanism will be designed to securely back up the private keys of IoT devices to another device, user or agent that it trusts and restoring them securely when required. The trust score of an IoT device is associated with its public key which intern is bound to its global and unique identifier. The risk and mitigation management method handles risks and when any abnormalities that lead to a harmful act happens, it informs the trust revocation mechanism to take actions. The risk mitigation and management system informs the trust revocation system to take proper actions on devices being identified ways to vulnerabilities and attacks in the IoT system. Depending on the level of identified risks the trust revocation system may revoke the trust score, public keys and identifiers and invalidate the verifiable claims of the victim devices.

IV. USE CASE SCENARIO: CAR RENTAL INDUSTRY

The car rental industry provides automobile renting services to customers on a temporary basis which may range from a few hours to months or as per kilometre basis. A customer could be a traveller, tourist, or individuals who don't have their own car. The global car rental market is growing following remarkable urbanization, world population growth, effect of environmental pollution, and high traffic congestion. This coupled with extensive industrialization, government restrictions regarding private car ownerships and high cost makes it difficult for individuals to buy and drive own car. The emergence of technologies such as smart phones and IoT is advancing the car rental industry. Existing car rental process is highly centralized relying mainly on the car rental companies which suffered from different attacks, single point of failure, limited scalability, and lack of information integrity. Moreover, the existing car rental industry involves laborious rental process, high costs and limited vehicle choice. Implementing a secure self-sovereign DLT based decentralized identity in the car rental industry enables fraud-proof, self-owned and controlled identities, eliminate central monopoly of all information and reduces the overhead cost. Moreover, the identifiers, verifiable credentials, consents and overall history of car rental companies, cars, customers, insurances, banks and other stakeholders are transparent and auditable in the DLT network. Finally, the DLT based decentralized self-sovereign IDMS generally brings improved service, reduced cost, easy monitoring, access and information sharing consistently about the identities of all participants of the DLT network. The architecture for this use case is shown in figure 2 below.

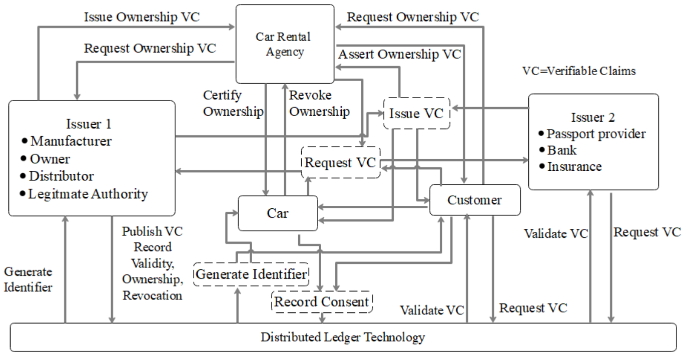

Fig. 2. Destributed, Secure SSI Mangement for Car Rental Industry Use Case

Figure 2 shows the high overview of the architecture for the car rental industry. It starts with device profiling (car), customer, car owner and other stakeholders detail registration (which could be optional if it is done already). Car rental agency, car owner, customer and the car generate an identifier from the blockchain and request verifiable identifiers from the issuers. The verifiable credentials can be a driving license, passport, bank account, insurance, certificate of ownership, and car's license plate number to mention some. Legitimate issuers provide the verifiable claim to the identity holders and are used for different services up on the verification by the service providers. Identifiers and verifiable claims are transparent and publicly verifiable in the DLT and sharing of identity information depends on the consent of the identity owner where they can fully or partially disclose them. Partial discloser can be not specifying the exact amount of money in the bank, and date of birth among many others. The trust score algorithm, risk mitigation and management, and trust revocation will be implemented as explained in III.

V. Conclusion

This study presents a novel solution which aims to overcome the identity management problems of devices in the IoT system. The traditional and current IDMSs which are not capable of addressing the current and growing demands of the identity management in the IoT ecosystem are addressed by the developed solution. This SSI based IDMS is implemented on the underpinning decentralized DLT technology, incorporating tangle technology. In the presented solution, IoT devices have full ownership and control over their identities via a portable, interoperable, persistent, secure and scalable system. This research has an ongoing active and future work with the following summary points: i) Device profiling compatible with DLT and SSI which include device enrolment, generating a unique identifier, device to identifier mapping, issuing, asserting and validating verifiable claims. ii) Analysis and design of trust score algorithm for IoT devices based on the web of trust, reputation and other factors. iii) Building risk mitigation and management that detects, identifies, categorizes and manages risks related to IDMS. iv) Developing a trust management system that revokes granted trust score, public keys, and associated identifiers based on mitigated and identified risks, life cycle and related issues of the IoT devices.

VI. References

1. Zhu X, Badr Y. Identity Management Systems for the Internet of Things: A Survey Towards Blockchain Solutions. Sensors (Basel). 2018;18(12):1–18.
2. International Telecommunication Union. Digital Identity Roadmap Guide. 2018.
3. Cao Y, Yang L. A survey of Identity Management technology. Proc 2010 IEEE Int Conf Inf Theory Inf Secur ICITIS 2010. 2010;287–93.
4. Grassi PA, Garcia ME, Fenton JL. Digital identity guidelines: revision 3. 2017; Available from: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf
5. Zhu X, Badr Y, Pacheco J, Hariri S. Autonomic Identity Framework for the Internet of Things. Proc - 2017 IEEE Int Conf Cloud Auton Comput ICCAC 2017. 2017;69–79.
6. Angrishi K. Turning Internet of Things(IoT) into Internet of Vulnerabilities (IoV) : IoT Botnets. 2017;1–17. Available from: http://arxiv.org/abs/1702.03681
7. Lin H, Bergmann N. IoT Privacy and Security Challenges for Smart Home Environments. Information [Internet]. 2016;7(3):44. Available from: http://www.mdpi.com/2078-2489/7/3/44
8. Nuss M, Puchta A, Kunz M. Towards Blockchain-based Identity and Access Management for Internet of Things in Enterprises.
9. Abraham A. Whitepaper Self-Sovereign Identity. 2017;1–39.
10. Axon L. Privacy-awareness in blockchain-based PKI. 2015; Available from: http://ora.ox.ac.uk/objects/uuid:f8377b69-599b-4cae-8df0-f0cded53e63b
11. Cooper D. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. [cited 2019 May 30]; Available from: https://tools.ietf.org/html/rfc5280
12. Jøsang A, Zomai M Al, Suriadi S. Usability and privacy in identity management architectures. Conf Res Pract Inf Technol Ser. 2007;68:143–52.
13. Ahmad Z, Sulaiman S, Iskandar BS, Manan JA. A study on threat model for federated identities in federated identity management system. 2010;(June 2014).
14. Bakre A, Patil N, Gupta S. Implementing Decentralized Digital Identity using Blockchain. 2017;4(10):379–85.
15. Jiang J, Duan H. A Federated Identity Management System with Centralized Trust and Unified Single Sign-On. 2011;(August).
16. Alpár G, Hoepman J-H, Siljee J. The Identity Crisis. Security, Privacy and Usability Issues in Identity Management. 2011;(May 2014). Available from: http://arxiv.org/abs/1101.0427
17. Vossaert J, Lapon J, Decker B De, Naessens V. User-centric identity management using trusted modules. Math Comput Model [Internet]. 2013;57(7–8):1592–605. Available from: http://dx.doi.org/10.1016/j.mcm.2012.06.010
18. Tuen CD. Security in Internet of Things Systems. 2015;(June).
19. GSMA. Distributed Ledger Technology, Blockchains and Identity. 2018;(September).
20. Bank W. Blockchain & Distributed Ledger Technology (DLT). World Bank [Internet]. 2018;(28). Available from: https://www.worldbank.org/en/topic/financialsector/brief/blockchain-dlt
21. Tobin A, Reed D. The Inevitable Rise of Self-Sovereign Identity. 2017;(March):23. Available from: https://sovrin.org/wp-content/uploads/2017/06/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf
22. Heck R, Torstensson J, Mitton Z, Sena M. Uport : a Platform for Self-Sovereign Identity. 2016;
23. Jacobovitz O. Blockchain for Identity Management. Tech Rep [Internet]. 2016;(December):1–19. Available from: https://www.cs.bgu.ac.il/~frankel/TechnicalReports/2016/16-02.pdf
24. To P, Telemetry P, Ci US. Autonomous Decentralized Peer-to- Peer Telemetry. 2017;1. Available from: https://patentimages.storage.googleapis.com/da/c9/5b/b17dbce7de523d/US20170310747A1.pdf
25. Ali MS, Vecchio M, Pincheira M, Dolui K, Antonelli F, Rehmani MH. Applications of Blockchains in the Internet of Things: A Comprehensive Survey. IEEE Commun Surv Tutorials. 2018;PP(November):1.
26. Popov S. IOTA whitepaper v1.4.3. New Yorker [Internet]. 2018;81(8):1–28. Available from: https://assets.ctfassets.net/r1dr6vzfxhev/2t4uxvsIqk0EUau6g2sw0g/45eae33637ca92f85dd9f4a3a218e1ec/iota1_4_3.pdf
27. Ioini N El, Pahl C. A Review of Distributed Ledger Technologies | SpringerLink.
28. Atlam HF, Wills GB. Intersections between IoT and distributed ledger [Internet]. 1st ed. Role of Blockchain Technology in IoT Applications. Elsevier Inc.; 2019. 1–41 p. Available from: http://dx.doi.org/10.1016/bs.adcom.2018.12.001
29. Markus Sabadello, Kyle Den Hartog, Christian Lundkvist, Cedric Franz, Alberto Elias, Andrew Hughes, John Jordan DZ. rwot6-santabarbara/did-auth.md at master · WebOfTrustInfo/rwot6-santabarbara · GitHub [Internet]. [cited 2019 Oct 29]. Available from: https://github.com/WebOfTrustInfo/rwot6-santabarbara/blob/master/final-documents/did-auth.md
30. Putra GD, Dorri A, Kanhere SS. A Trust Architecture for Blockchain in IoT.