Privacy Preserving Issues in the Dynamic Internet of Things (IoT)

Áine MacDermott[1], John Carr[1], Qi Shi[1], Mohd Rizuan Baharon[2], and Gyu Myoung Lee[1]
[1]*Department of Computer Science, Liverpool John Moores University, Liverpool, UK*
[2]*Department of Computer System and Communication, Universiti Teknikal Malaysia, Melaka, Malaysia*
[1]{a.m.macdermott, j.j.carr, q.shi, g.m.lee}@ljmu.ac.uk [2]mohd.rizuan@utem.edu.my

***Abstract*— Convergence of critical infrastructure and data, including government and enterprise, to the dynamic Internet of Things (IoT) environment and future digital ecosystems exhibit significant challenges for privacy and identity in these interconnected domains. There are an increasing variety of devices and technologies being introduced, rendering existing security tools inadequate to deal with the dynamic scale and varying actors. The IoT is increasingly data driven with user sovereignty being essential – and actors in varying scenarios including user/customer, device, manufacturer, third party processor, etc. Therefore, flexible frameworks and diverse security requirements for such sensitive environments are needed to secure identities and authenticate IoT devices and their data, protecting privacy and integrity. In this paper we present a review of the principles, techniques and algorithms that can be adapted from other distributed computing paradigms. Said review will be used in application to the development of a collaborative decision-making framework for heterogeneous entities in a distributed domain, whilst simultaneously highlighting privacy preserving issues in the IoT. In addition, we present our trust-based privacy preserving schema using Dempster-Shafer theory of evidence. While still in its infancy, this application could help maintain a level of privacy and nonrepudiation in collaborative environments such as the IoT.**

Keywords—internet of things, iot, privacy, security, trust, blockchain, decision making, dempster-shafer.

I. INTRODUCTION

The Internet of Things (IoT) landscape is fragmented with a large variety of devices and technology. The term IoT is used to describe collections of Internet-enabled 'things' or smart devices, increasingly interconnected with other 'things' in a mass ecosystem [1]. Similarly, the Industrial Internet of Things (IIoT) describes industrial 'things' where the end devices typically comprise sensors, actuators and industrial processes, used for automation and data collection. In combining machine-to-machine communication with industrial big data analytics, IIoT is driving unprecedented levels of efficiency, productivity, and performance. With the increasing utilisation of 'things' for business and automation, industries have access to greater insight and real-time operational awareness with methodical data generation. The IoT has made an enormous quantity of data available, belonging not only to consumers, but to citizens in general, groups, and organisations [2]. IoT data is becoming one of the most valuable assets in today's data-driven digital economy as it leads to developing many business models providing ubiquitous and intelligent services. However, this data contains sensitive personal information and can reveal the identity of the associated stakeholders if appropriate privacy preserving mechanisms are not in place [3].

Technology is increasingly being utilised in conjunction with the IoT for improved performance, security, and improved trust. One such application for privacy preservation is Blockchain. Blockchain technology has been around for just under a decade, initially introduced as a way to store and/or send the first cryptocurrency, Bitcoin. As the technology has gradually spread worldwide, it has been used in a variety of ways in numerous industries, including the increase of cybersecurity measures and resilience. Capabilities of the blockchain technology, including trustworthiness, decentralization, scalability, and autonomy, make it a potentially essential component of the overall IoT ecosystem. The main benefit lies in the decentralized immutable and verifiable ledgers that can record transaction of digital assets. Once recorded, data in any given block cannot be altered retroactively as this would invalidate all hashes in the previous blocks in a blockchain and break the consensus agreed among nodes voiding said blockchain [3]. Open research challenges relating to privacy-preservation include transaction cryptographic key management, interoperability among dynamic devices and entities and compliance with privacy regulations such as General Data Protection Regulation (GDPR) [4].

Interoperability issues among devices and friction for data flow is a challenge that can lead to poor data quality or misinformation. GDPR conveys the importance of a "privacy by design" concept which essentially calls for privacy to be considered throughout the whole engineering process. While the principles of data accountability and transparency were previously subject to implicit requirements of data protection law, GDPR further extends the requirements of authorities by introducing explicit provisions that promote data accountability and governance to protect the privacy of data. GDPR defines three participant roles: the Data Subject (DS), the Data Controller (DC), and the Data Processor (DP), while specifying their associated obligations under EU data protection law [3].

The contributions of our work are as follows; we present a review of privacy preserving issues in the IoT, as well as the related technologies and prevailing approaches at present. We also convey our trust-based privacy preserving schema using Dempster-Shafer (D-S) theory of evidence. D-S theory introduces the concept of assigning beliefs and plausibility to possible hypotheses of each decision maker (for example, in this scenario it represents the view of the aforementioned participant roles, DC/DP), and provides a combination rule to fuse multi-modal information to aggregate and summarise a relevant body of evidence. The remainder of this paper is as follows: In Section II we provide background to the IoT and associated privacy issues. Section III explores related works in the area of privacy preservation in the IoT. In Section IV we detail our proposed Trust-based preserving schema using

978-1-7281-5628-6/20/$31.00 ©2020 IEEE

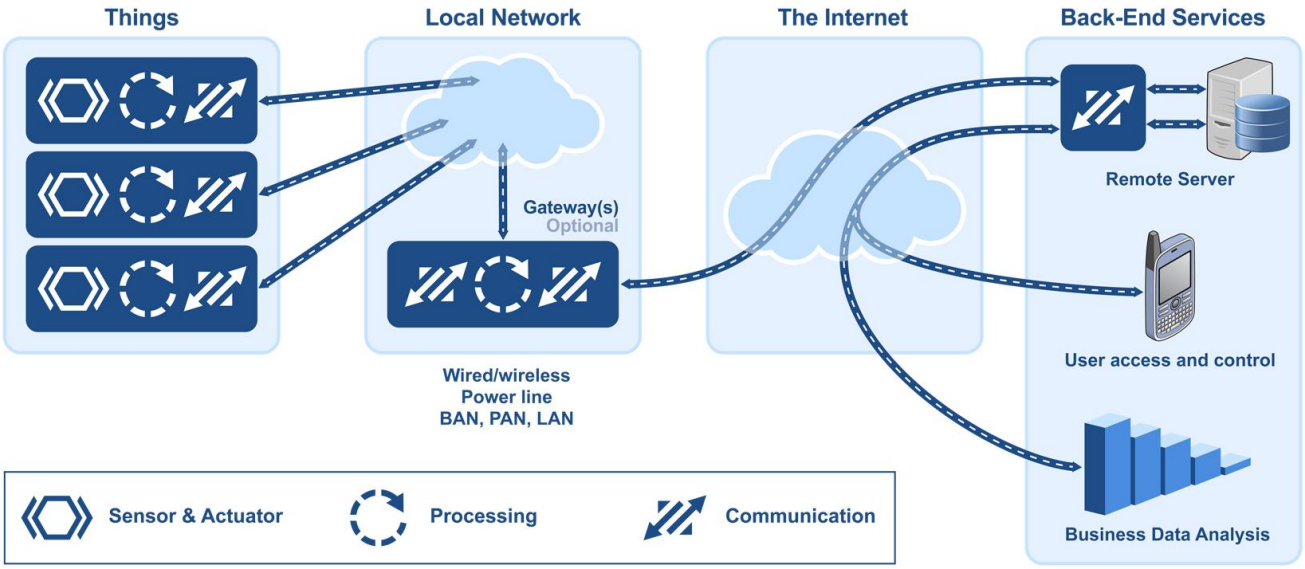

Fig. 1. The Internet of Things from an embedded systems point of view

Dempster-Shafer theory of evidence, offering insight and discussion of the research problem in Section V. Conclusions are presented in Section VI.

II. Background

The Internet of Things (IoT) is not a new paradigm; the technological capabilities of society have enabled its immense progression and increased utilisation. The mass of devices and complex ecosystems has given rise to the terms "The Internet of Anything/Everything" [5, 6], leading to the need for a "Web of Things": an Internet created to be more compatible with IoT devices. At present, IoT devices are not strongly standardized in how they are connected to the Internet, apart from their networking protocols [6]. Rather, they create a wider attack surface with billions of new devices. This mass exchange of information between nodes opens up privacy concerns – especially in public applications. We aim to empower data provenance and transparency by leveraging advanced features of the emerging technologies (e.g., Blockchain) for privacy preservation in the IoT environment and corresponding applications.

A high level overview of the IoT and associated attributes is given in Figure 1 [4]. IoT systems consist of four main features: 1) The things (devices), 2) Local network (wired/wireless with an array of topologies), 3) The Internet, and 4) Data storage applications/Back-end services (e.g. user access and control, data analytics, remote server management etc.). The communication and transmission of devices can differ depending upon the environment. For example, a commercial IoT device will communicate with other local devices via Bluetooth or Ethernet (wired or wireless), whereas an IIoT device may comprise a local network with many different technologies, so the device would typically transmit data over the Internet. The IoT presents several unique challenges that make the application of existing security and privacy techniques difficult. This is because IoT solutions encompass a variety of security and privacy solutions for protecting such IoT data on the move and in store at the device layer, the IoT infrastructure/platform layer, and the IoT application layer [5]. This is not sufficient if the endpoints themselves are vulnerable to modification by either local access or remote connections [6]. Additionally, encryption algorithms require higher processing power than many of the IoT devices possess.

Data security and privacy issues are an increasing concern due to the wealth of data collected, stored, and processed on IoT-based devices. Depending on the nature of the device, this data can take the form of personalised, location specific, or user-centric information. As conveyed in the introduction, the IoT is increasingly data driven – actors in each varying scenario including the user/customer, the device, manufacturer, third party processor, etc. The issue of anonymity in the IoT is important to note also. While a challenge to provide, there may be an increasing desire for anonymity, which directly clashes and contrasts with desire for an increased level of service, as personalised data often requires understanding to 'whom' the service is being provided [2]. User sovereignty, with regards to security, privacy and trust is a key concern when discussing the IoT. The IoT will become an "Internet fabric", where everything is digitally connected as a normal integrated part of society like electrical grid or water supply.

Privacy issues within the IoT can be summarised as follows:

- User Identification: The IoT includes a huge number of interactive nodes that generate, accumulate and exchange sensitive data. Usage of pseudonyms avoids linking transactions to the real identities, though users and consumers are not completely anonymous in their movements. Pseudonyms may be traceable and linkable as various accounts or 'things' may belong to the same user [7].
- User tracking/User profiling/Utility monitoring: Big data analytics is imperative for dealing with the volume of generated data. Data is collected from users behaviours and routines through interaction with 'things', which is then analysed and processed to create useful information for predictive analytics. Real-time monitoring based on the information gathered from the connected 'things' provides large scale connectivity and a greater insight into individual habits and routines [1]. This collected data can increase

privacy concerns with data subjects, data controllers, and data processors.

- Multi-platform/services: as devices are interconnected with various hardware and software the risk of sensitive information leaking through unauthorized access/manipulation increases. Malicious data and entities could affect and ruin the whole chain.

The highly diverse IoT application domains, resource-constrained IoT devices, and heterogeneity of both devices and platforms hinder the development of a standard IoT framework. The security data of domestic IoT platforms is not much considered as compared with the international IoT platforms. An IoT standard platform that can interoperate with all IoT platforms is needed, with interoperability issues being key for future developments. However, privacy stands out as a critical concern that inhibits the widespread adoption of IoT. The underlying vulnerabilities of IoT devices can lead to huge security breaches and significantly hurt user privacy by exposing personal data [8]. Privacy needs to be "by design" whereby the management of such heterogeneous entities in a distributed domain can be addressed at the design stage. Legislation should be adjusted and addressed accordingly, with a multi-faceted approach between industry and policy makers utilising realistic use cases and scenarios for application.

III. Related Work

A. Blockchain

Blockchain deployments are increasingly being utilised in e-government, e-health, smart cities, critical infrastructure services, and cryptocurrencies. As conveyed in [9], the ability to maintain a decentralized trusted ledger of all transactions occurring in a network is an encouraging attribute of blockchain technology. This capability is essential to enable the regulatory requirements of IoT/IIoT applications without the need to rely on a centralised model. Blockchains also provide participants with enhanced transparency, making it much more difficult to corrupt blockchains through malware or manipulative actions, and may contain multiple layers of security – both at the network level and installed at the level of each individual participant [10]. Blockchain-based techniques offer strong countermeasures to protect data from tampering while supporting the distributed nature of the IoT. However, the enormous amount of energy consumption required to verify each block of data makes it difficult to use with resource-constrained IoT devices, and with real-time IoT applications [3]. The delay associated with the mining process is not suitable for real-time IoT applications, in addition to scalability issues associated with blockchain, and further overhead created by blockchain consensus algorithms. Scalability is a further issue with this integration. With the amount of transactions increasing day by day, the blockchain becomes unwieldly. Each node has to store all transactions to validate them on the blockchain, as they have to check if the source of the current transaction is unspent or not [11].

By nature, blockchain technology is inherently resistant to data modification due to its public ledger and the consensus mechanism called Power of Work (PoW). Once recorded, data in any given block cannot be altered as this would invalidate all hashes in the previous blocks in a blockchain and break the consensus agreed among nodes voiding said blockchain. Blockchain technology is considered the key solution to solve privacy and reliability issues in the IoT [9]. It can be used in tracking billions of connected devices, enabling the processing of transactions and coordination between devices. All blocks within a Blockchain will contain its own digital signature, the previous blocks digital signature, and its content data. Each digital signature is calculated from the previous digital signature, and if a previous blocks data is changed then its signature will also change, in turn impacting the signatures of all following blocks. The calculation and comparison of signatures allows us to identify if any blocks within a chain are invalid. Additionally, consensus mechanisms improve the overall robustness and integrity of shared ledgers, because consensus among network participants is a prerequisite to validating new blocks of data, and mitigates the possibility that a hacker or one or more compromised network participants can corrupt or manipulate the ledger [10].

B. Trust

Benefits of a collaborative monitoring scheme include greater efficiency and increased monitoring accuracy, which are a result from the collective pooling of resources for a single purpose [12]. Trust management is an effective method to identify malicious, selfish or compromised nodes [13]. The current trust evaluation schemes aim to improve detection performance, resource efficiency, robustness etc., by using fuzzy theory, probability theory and statistics, weighting method, and so on. In Atakli et al. [14], a weighted-trust evaluation based scheme was proposed to detect compromised or misbehaved nodes in WSNs by monitoring their reported data. The hierarchical network can reduce the communication overhead between sensor nodes by utilizing clustered topology. By comparing the trust value with predefined thresholds, they can decide whether the sensor node is compromised or not.

Arachchilage et al. [15] convey the importance of collaborative parties having an established guarantee about the type of information they will be sharing in order to protect sensitive information. They identify data, policy, controls, roles, actions and evidence as being fundamental concepts for building a trust domain. Their research aims at managing trust related issues in information sharing schemes via development of measurable trust characteristics. Future avenues aim at supporting collaboration and data exchange within and across multiple organisations by developing a mechanism to represent Trust Domains, supporting tool integration and decision-making based on the integration of evidence from different sources.

The work of Wang et al. [16] proposes the use of D-S theory of evidence to fuse local information and make a system wide decision. Each monitoring agent collects information in its local domain, then generates a decision based on an observation, serving as evidence. As a basic probability assignment function (BPAF) and its corresponding frame of discernment are called a body of evidence, each sensor therefore corresponds to said body of evidence. The essence of multi-sensor data fusion is that within the same frame of discernment, different bodies of evidence (depending on fusion rules and feature thresholds), are fused into a resultant BPAF, on which the system makes the final decision based on decision rules. While this shows successful application of the D-S combination, this can be environment specific. The metrics are application dependent; where the output space of a system is large and the probability of producing identical incorrect redundant results is low, the number of agreed results, during a specific running time, is a

suitable metric. If the cardinality of voter output space is small and identical, and incorrect redundant results are probable, then the number of agreed and correct results is a suitable metric [12]. The ratio of correct results to agreed results may be the most suitable measure. Unavoidably, voter reputation and ranking may change when using different metrics. Examples of typical metrics used include the probability of producing a correct voter output, error detection ratio, and the number of normalised benign outputs, to name a few [17].

C. Interoperability and Semantics

The IoT landscape is fragmented: the diversity, volatility, and ubiquity make the task of processing, integrating, and interpreting real world IoT data a challenging task. In order to develop interoperable IoT applications that can detect events in the real world and respond accordingly, deducing knowledge from gathered raw data is a prerequisite. Al-Osta et. al [18] proposed a lightweight semantic web-based approach for data annotation focusing on IoT gateway data. In [12], they detail how semantic web technologies have been extensively utilised to interpret and integrate data coming from numerous resources; recently being extended to the IoT domain to enhance the quality of data and to promote interoperability. This is achieved by modelling IoT data based on shared vocabularies that can be interpreted by different software agents. While this application and interpretation of raw data has its merits, concerns remain regarding the lack of data preparation and filtering mechanisms, which dictates that the edge/gateway devices have to process and annotate all the data regardless of its importance to the context of an application, therefore increasing resource consumption and network traffic between the cloud and the gateway.

Semantic interoperability means that different stakeholders can access and interpret the data unambiguously. The "Things" in the IoT need to exchange data among each other and with other users on the Internet. Providing unambiguous data descriptions in a way that can be processed and interpreted by machines and software agents is a key enabler of automated information communications and interactions in IoT [19]. A context-based security and privacy approach is proposed in [20]. Through modelling service and data flow, their security architecture applies separation of concerns between end point 'things', and external 'things' who manage or use the services. Intelligent Trusted Authority (ITA) facilitate and apply policies modelled by the supervisory system and big data elements, with external flows screened by an authorisation unit. Access and flow conditions via authentication and least privilege per entity of the architecture are proposed and conveyed in a conceptual framework. The web and the semantic web are the most significant cases of environments where the information is distributed. In parallel, we observed the rise of blockchain as a way to distribute assets and trust in recent years.

D. Regulations

The European Union Agency for Cybersecurity (ENISA) report "Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures" [21] ranked attack scenarios in terms of criticality on an IoT environment. Two that stand out and convey a high loss in terms of trust, security and privacy are "*IoT administration system compromise*" and "*Value manipulation in IoT devices*". 'IoT administration system compromise' conveys how infections can be designed to take control over one or multiple IoT devices, in order to manipulate or crash them and to be able to modify values, change their functioning/behaviour or deny access to them. Since a compromised administration system leads to several assets being compromised over a long period of time and without being detected, the impact of this attack can be critical.

Assets affected include 'things', data, gateways, devices to interface with 'things' and devices to manage 'things'. The attack scenario 'Value manipulation in IoT devices' uses an IIoT device to detail how manipulation of calibration parameters for the sensors allows undesired values to be accepted when they should not, which poses a severe threat to critical systems and integrity of system data. This attack targets the sensor processing and knowledge model levels of the control system - by allowing the sensors to report and accept incorrect values, the IoT environment is put at high risk. The assets affected include sensors, actuators, decision making, and sensitive data. The work in "Privacy-Preserving Solutions for Blockchain: Review and Challenges" [7] is a good resource for distinguishing participant roles: Data Subject (DS), Data Controller (DC), and Data Processor (DP). Although the use cases are specific to attacks in industry, different industries often use tailored security enablers and a wide variety of tools and technologies. This point is addressed though, as while the report has evident merits, it goes on to state: "*fragmentation of the regulations also poses a barrier when Critical Information Infrastructures are seen hand in hand with the IoT world, since there is no regulation that forces security measures and protocols in the different levels of an IoT ecosystem, including the devices, the network, etc."* Regulations, standards and best practices are key for devices to be one less vulnerable entity in the whole ecosystem. Security and management of devices worldwide would help ensure a consistent approach to IoT security and privacy.

IV. Privacy Preserving Decision Making

Our application focuses on privacy preserving mechanisms and autonomous decision making in distributed schemas. In the IoT, decision making often occurs on the edge of the network, via monitoring agents or by monitoring IoT device trustworthiness. While numerous applications and approaches exist that can be applied to the environment, one of the key challenges is interoperability. How do we ensure that the data we collect is correct? If said data is incorrect then we are basing decisions on misinformation. As identified in the related work section, there are numerous models exploring privacy preservation in IoT via trust verification models, user authentication schemes via identity methods and risk scoring to determine likelihood etc., but what is apparent is that blockchain encompasses these attributes in one solution: discovery, trust, data identity/management. While our approach remains in the preliminary stages, we are focusing on the decision-making approaches taken by these algorithms and frameworks at present.

Within this section, our Trust-based preserving schema using D-S theory of evidence is proposed, whereby we apply said theory to a collaborative infrastructure as a whole, with an underlying IoT environment. We also assume that this decision-making and processing will occur on the Edge/Fog layer on the environment, providing an inferencing engine for prediction and quick action. D-S theory of evidence is a probabilistic approach, which implements belief functions which are based on degrees of belief or trust [12]. For example, other decision-making schemes utilise a simple majority vote for group consensus and the final decision is

binary. By adopting a vector-based voting solution the failure rate in these schemes can be significantly reduced compared to non-vector voting by about 50% [17]. If a voter is a Boolean (YES/NO) decision maker, its output space is binary; and if the output of a vote can be of any value, its output space is infinite. The majority vote decision making process produces an output among variant results, where at least (n+1)/2 variant results agree. However, the disadvantage of the widely used majority vote is that they may agree on incorrect variant results, where there is a consensus on identical incorrect inputs - these voters cannot distinguish between agreed correct and agreed incorrect variant outputs. The majority vote is often inaccurate, especially in automated approaches. The task of aggregating the different votes/decisions into a single result and deciding about the observed events remains a challenge. By contrast, D-S produces a judgement value between 0 and 1 that reflects the degree of belief in that judgement [23].

The monitoring system we propose is faced with the task of aggregating different outputs into a single result, making a decision about the observed events. For example, each feature *(f ∈ F)* describes the type of information, and *V* defines the range of possible values of the feature. Given an event and monitoring agent identity, a local report R_{Local} is defined as a tuple consisting of <*eid, ts, g, (f, v), p*> where: *eid* is a unique event identifier, *ts* is the events timestamp, g ∈ G is the agent's identity, *(f, v)* is a feature-value pair corresponding to the output of the data collection action performed by agent *g*. The agent's analysis of the activity is p ∈ [0, 1]; i.e. the probability of the activity being suspicious or malicious [22]. This output of activity is represented as a belief function represented as a hypothesis of events. Agent based monitoring and clustering can improve overall accuracy, with trust in connected nodes being a major challenge.

D-S utilises orthogonal sum to combine the evidences, where ⊕ is the combination operator. The belief functions are defined, describing the belief in a hypothesis A , as $\mathrm{Bel}_1(\mathrm{A}), \mathrm{Bel}_2(\mathrm{A})$; then the belief function after the combination is defined as:

$$\mathrm{Bel}(\mathrm{A}) = \mathrm{Bel}_1(\mathrm{A}) \oplus \mathrm{Bel}_2(\mathrm{A}) \tag{1}$$

The mass function after the combination can be framed as:

$$\mathrm{m}(\mathrm{A}) = \mathrm{K}^{-1} . \sum_{\mathrm{A_i} \cap \mathrm{B_i} = \mathrm{A}} \mathrm{m}_1(\mathrm{A_i})\, \mathrm{m}_2(\mathrm{B_j}) \tag{2}$$

Here, *K* is called the Orthogonal Coefficient, and it is defined as:

$$\mathrm{K} = \sum_{\mathrm{A_i} \cap \mathrm{B_i} \neq \emptyset} \mathrm{m}_1(\mathrm{A_i})\, \mathrm{m}_2(\mathrm{B_j}) \tag{3}$$

D-S combines the beliefs expressed by monitors to produce a single combined belief that is finally compared with a set accumulative sum q of beliefs. Assuming that two Basic Probability Assignments (BPAs) m^a and m^b represent the beliefs about values of a state within a specific frame θ the use of the orthogonal coefficient in Equation 2 and normalization in Equation 3 conveys that D-S is mathematically possible only if m^a and m^b are not conflicting, i.e. if there is a focal element y of m^a and a focal element z of m^b satisfying the intersection (∩) of the two sets, $(y \cap z) \neq \emptyset$, so that they have no elements in common. Merging two belief masses with the conjunctive rule produces a sub-additive BPA, meaning that the sum of belief masses on focal elements can be less than one. Thus, it is assumed that the missing or complement belief mass gets assigned to the empty set. If required, the normality assumption m(∅) = 0 can be recovered by dividing each belief mass by a normalization coefficient [24]. Furthermore, this rule is associative.

The normalisation stage in D-S's rule redistributes conflicting belief masses to non-conflicting ones, and tends to eliminate any conflicting characteristics in the resulting belief mass distribution. This rule of combination can be applied to avoid this particular problem by allowing all conflicting belief masses to be allocated to the empty set. The order of the information in the aggregated evidences does not impact the result, however a non-associative combination is necessary for many cases. Application of this rule combination implies that all evidence is trusted equally, with the same confidence in their results, and that all sources have the same level of trust. In reality, the confidence and trust depending upon source or observer or upon different evidence may differ. As such, various factors for all evidences should be considered, and adjusted as needed with the ability to score or rate decisions [12].

There should be a way to overrule the decision based on the strength of the associated trust or confidence value associated with the decision. Post Belief generation processing may be applied to this area to facilitate information exchange for defence. Via the inclusion of confidence values when Belief generation occurs, the accuracy of decisions can be improved, with the inclusion of confidence values and trust scores helping to resolve the issue with equality on opinion in the fusion stage. Let $P^{(a)} = [P_1^{(a)} \ldots P_{Ka}^{(a)}]$ denote the K_a possible confidence values G associated with choosing $a \in A$ at time t_d. The assigned confidence level $p \in P^{(a)}$ associated with deciding a after waiting for a period of $t_c = t_d + \tau$ is given as [25]:

$$p = P_1^{(a)} \text{ when } L(t_c) \in \left[G_{i-1,}^{(a)} G_i^{(a)}\right], \tag{4}$$

where $G_0^{(a)} = -\infty$ and $G_{Ka}^{(a)} = \infty$ for each $a \in A$, and the value τ is known as the inter-judgement time.

The remaining confidence parameters:

$$G^{(a)} = [G_1^{(a)} \ldots G_{Ka-1}^{(a)}] \tag{5}$$

are chosen such that $G_{i-1} < G_i$ for each $i \in \{1 \ldots \ldots, K_a - 1\}$.

Adding a degree of confidence to each generated belief can improve the overall efficiency, and deal with the issue of conflicting beliefs during fusion. While significant research into reputation-based approaches and levels of trust attributes is ongoing, the underlying semantics are only as smart as the data it holds and processes.

V. Conclusions

The IoT is rapidly becoming an Internet "Web of Things", and there is an increasing need for technologies to expand at the same rate. Data is the most valuable asset in this interconnected paradigm, and protecting privacy becomes increasingly difficult as the IoT becomes more prevalent in future. Such an increase in connectivity and data collection results in less control, both of the data and of the devices that are connected. There is a need for a well-defined trust model for IoT applications, where the trust score is a performance metric based on functional properties relevant to the collaboration context. We have presented our trust-based

preserving schema using D-S theory of evidence, offering significant improvements over current decision-making algorithms whereby the inclusion of confidence values and reputation scores can reduce the risk of 51% attacks in the blockchain. While research into the reputation-based scoring and levels of trust attributes is ongoing, the underlying semantics require adaptation to the relevant environment. A performance evaluation of the framework will be carried out as part of future work, comparing said framework with the trust-based schemes mentioned in the related works section. Blockchain technology offers a promising route for maintaining integrity of data and providing an irreversible chain of evidence, as well as distributing assets and trust. However, the ever-increasing fragmentation and diversity of the IoT landscape may pose problems for the future integration of blockchain in the IoT; therefore, while it may seem promising, it cannot work on all scenarios at present. Future research is needed in order to properly assess, mitigate and counter these problems with relevant use cases.

REFERENCES

[1] Á. MacDermott, P. Kendrick, I. Idowu, M. Ashall, and Q. Shi, "Securing things in the healthcare internet of things," Global IoT Summit, GIoTS 2019 - Proceedings, 2019.

[2] C. Maple, "Security and privacy in the internet of things," Journal of Cyber Policy, vol. 2, no. 2, pp. 155–184, 2017.

[3] U. Jayasinghe, G. M. Lee, Á. MacDermott, W. S. Rhee, and K. Elgazzar, "TrustChain: A Privacy Preserving Blockchain with Edge Computing," Wireless Communications and Mobile Computing, vol. 2019, 2019.

[4] Micruim, "Designing the Internet of Things," 2019 Silicon Labs, 2020. [Online]. Available: https://www.micrium.com/iot/devices/.

[5] P. P. Jayaraman, X. Yang, A. Yavari, D. Georgakopoulos, and X. Yi, "Privacy preserving Internet of Things: From privacy techniques to a blueprint architecture and efficient implementation," Future Generation Computer Systems, vol. 76, pp. 540–549, 2017.

[6] W. M. S. Stout and V. E. Urias, "Challenges to Securing the Internet of Things," in 2016 IEEE International Carnahan Conference on Security Technology (ICCST), 2020, pp. 1–8.

[7] J. Bernal Bernabe, J. L. Canovas, J. L. Hernandez-Ramos, R. Torres Moreno, and A. Skarmeta, "Privacy-Preserving Solutions for Blockchain: Review and Challenges," IEEE Access, vol. 7, pp. 164908–164940, 2019.

[8] M. Seliem, K. Elgazzar, and K. Khalil, "Towards Privacy Preserving IoT Environments: A Survey," Wireless Communications and Mobile Computing, vol. 2018, no. October 2016, 2018.

[9] H. F. Atlam, A. Alenezi, M. O. Alassafi, and G. B. Wills, "Blockchain with Internet of Things: Benefits, challenges, and future directions," International Journal of Intelligent Systems and Applications, vol. 10, no. 6, pp. 40–48, 2018.

[10] E. English, A. D. Kim, and M. Nonaka, "Advancing Blockchain Cybersecurity : Technical and Policy Considerations for the Financial Services Industry," Cybersecurity policy and resilience, p. 24, 2018.

[11] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," Proceedings - 2017 IEEE 6th International Congress on Big Data, BigData Congress 2017, no. June, pp. 557–564, 2017.

[12] M. Al-Osta, B. Ahmed, and G. Abdelouahed, "A Lightweight Semantic Web-based Approach for Data Annotation on IoT Gateways," Procedia Computer Science, vol. 113, pp. 186–193, 2017.

[13] P. Barnaghi, W. Wang, C. Henson, and K. Taylor, "Semantics for the internet of things: Early progress and back to the future," International Journal on Semantic Web and Information Systems, vol. 8, no. 1, pp. 1–21, 20pe12.

[14] V. Alagar, A. Alsaig, O. Ormandjieva, and K. Wan, "Context-based security and privacy for healthcare IoT," Proceedings - 2018 IEEE International Conference on Smart Internet of Things, SmartIoT 2018, pp. 122–128, 2018.

[15] Á. MacDermott, "Collaborative Intrusion Detection in Federated Cloud Environments using Dempster-Shafer Theory of Evidence," 2017.

[16] J. Wang, S. Jiang, and A. O. Fapojuwo, "A protocol layer trust-based intrusion detection scheme for wireless sensor networks," Sensors (Switzerland), vol. 17, no. 6, 2017.

[17] I. M. Atakli, H. Hu, Y. Chen, W. S. Ku, and Z. Su, "Malicious node detection in wireless sensor networks using weighted trust evaluation," Proceedings of the 2008 Spring Simulation Multiconference, SpringSim'08, pp. 836–843, 2008.

[18] N. Asanka, G. Arachchilage, C. Namiluko, and A. Martin, "A taxonomy for securely sharing information among others in a trust domain," in 8th International Conference for Internet Technology and Secured Transactions (ICITST), 2013, pp. 296–304.

[19] Y. Wang, H. Yang, X. Wang, and R. Zhang, "Distributed intrusion detection system based on data fusion method," in 5th World Congress on Intelligent Control and Automation, 2004, pp. 4331–4334.

[20] G. Latif-Shabgahi, J. M. Bass, and S. Bennett, "A Taxonomy for Software Voting Algorithms Used in Safety-Critical Systems," IEEE Transactions on Reliability, vol. 53, no. 3, pp. 319–328, 2004.

[21] European Union Agency for Cybersecurity (ENISA), Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures, no. November. 2017.

[22] P. Kendrick, A. Hussain, N. Criado, and M. Randles, "Multi-agent systems for scalable internet of things security," in Proceedings of the Second International Conference on Internet of things, Data and Cloud Computing, 2017, pp. 88–93.

[23] T. M. Chen and V. Venkataramanan, "Dempster-Shafer theory for intrusion detection in ad hoc networks," IEEE Internet Computing, vol. 9, no. 6, pp. 35–41, 2005.

[24] A. Josang and S. Pope, "Dempster's Rule as Seen by Little Coloured Balls," Computational Intelligence, vol. 28, no. 4, pp. 453–474, 2012.

[25] D. J. Bucci, S. Acharya, T. J. Pleskac, and M. Kam, "Subjective confidence and source reliability in soft data fusion," in 48th Annual Conference on Information Sciences and Systems, (CISS 2014), 2014, pp. 1–6.