Proceedings of the 25th International Conference on Automation & Computing, Lancaster University, Lancaster UK, 5-7 September 2019

Secure Data Aggregation Mechanism for Water Distribution System using Blockchain

Haitham Hassan M. Mahmoud
School of Engineering and Built Environment
Birmingham City University
Birmingham, United Kingdom
Haitham.Mahmoud@bcu.ac.uk

Wenyan Wu
School of Engineering and Built Environment
Birmingham City University
Birmingham, United Kingdom
Wenyan.Wu@bcu.ac.uk

Yonghao Wang
School of Computing and Digital Technology
Birmingham City University
Birmingham, United Kingdom
yonghao.wang@bcu.ac.uk

***Abstract*— Development of intelligent systems in particular Water Distribution Systems (WDS) increases the demand of implementing a secure scheme that can preserve user's identification and data consumption through maintaining confidentiality, authentication and integrity. Decentralization topology has investigated a lot recently in the literature with the development of bitcoins and Ethereum networks in different IoT disciplines such as power systems and healthcare systems. In this paper, feasibility and uses cases studies on the integration WDS with Blockchain Technology are discussed. Moreover, the customer's data and identity anonymity techniques that can be integrated with the network are discussed. Furthermore, a data aggregation mechanism of the smart meters in Water Distribution System (WDS) based on distributed ledger and Blockchain technologies is proposed. Further, the customer's identity using bloom filter is simulated and optimal parameters of the bloom filter are suggested.**

Keywords-Water Distribution System; Smart Water Network; Blockchain, Secure Scheme

I. INTRODUCTION

Water networks are one of the critical infrastructure's essentials for human life and health since they can affect the safety and health well-being of the citizen, the fact is that they can be endangered, disrupted by physical or cyber threats. Therefore, it is important to continuously monitor and control these networks to minimize the potential of attacks either on operational technology (OT) or information technology (IT). Also, it ensures a quality, efficient, robust, and reliable process of the whole network. This can be conducted by implementing a Smart Water Network (SWN) along with a secure scheme that can stand against cyber-attacks.

Water utility services oversee the sensitive personal information of the users' and employees' records as well as their payments information. There are several examples of cyber-attacks in the water sector such as; the ransom-ware attack in the city of Atlanta in March 2018 where the watershed management employees were unable to log in the system for two weeks and the utility had to take the servers down for months with an estimated $5 million in recovery efforts [1]. Cybercriminals have accessed customer data through the online payment system where the attackers have got the administrator credentials [2]. Also, they have gained access to valves and flow operations according to the American Water Works Association (AWWA) [3]. A 2018 study [4] showed that for every sixty seconds the cyber-crime costs more than $1.1 million and impacts more than 1,800 people. Water sectors are warned by the U.S. government of similar attacks that occurred led to shutting down Ukraine's power grid in Dec-ember 2015 [5]. American National Standards Institute (ANSI) American Water Works Association (AWWA) have released several standards in security Practices for Operation & Management [6], Risk & Resilience Management of Water & Wastewater Systems [7], and Emergency Preparedness Practices [8]. The water sector in the United Kingdom (U.K.) has only witnessed one cyber-attack in 2017 on National Health Service (NHS) where hackers managed to shut down hundreds of computers in health service demanding a ransom payment. This attack caused the cancellation of more than 19,000 appointments with an estimation loss of £92 million [9]. Also, with the development of SWN devices in the internet of things (IoT) environment will open more avenues for hackers as it happened in Ukraine in the power grid system.

Moreover, according to [10], 70% of the world's power, water, and other critical infrastructure utilities reported a cyber-attack within one year, while 78% of these attacks are expected to be succeeded breaching in the next two years. Moreover, the water crises have been ranked as the fifth of the top risks in terms of impact according to the World Economic Forum Global Risks Perception Survey 2018 [11]. Water crises have more than average impact and the more average likelihood or global risks. Located Furthermore, the number of reported cybersecurity in the water domain has been increasing in the last couple of years. According to Schneider Electric [12], 4% and still increasing of the reported cyber-attacks incidents are in the water domain in the United States (U.S.) in 2017. Further, according to [13] the attacking events, in general, are increasing rapidly from 2017 to 2018 where it can reach 130 events in a month instead of 80.

High-security level, is established by working of the OT such as; SCADA, PLC, Pumps etc… and IT such as processing platforms, etc…. A global survey in 2012 which is released by Sensus [14] showed data from SWNs that using similar networks can save utilities up to $12.5 billion per year and it will help to ensure a balance between the supply and demand. Estimated of $9.6 billion each year is the amount of water leakage stated in the Sensus survey [14]. Furthermore, it is expected that two-thirds of the world population or 4.6 billion people will suffer from stressed conditions of water resources.

Recently, literature has been discussing integrating distributed ledger and smart contracts in Blockchain

technology with IoT devices in smart homes [15, 16], smart cities [17], healthcare [18, 19], and power grid systems [20]–[22]. Integrating Blockchain with Water networks is not investigated in the literature. The work in this paper is inspired by the work in [22].

The main contribution of this paper is to explore the feasibility and uses cases studies on integrating Blockchain technology with smart water networks. Moreover, the customer's data and identity anonymity techniques that can be integrated with the network are discussed. Furthermore, a data aggregation mechanism of the smart meters in Water Distribution System (WDS) based on distributed ledger and Blockchain technologies is proposed. Further, customer's identity using bloom filter is simulated and optimal parameters of the bloom filter is suggested.

This paper is organized as follows: Section II explores the feasibility and uses cases on integrating Blockchain in Smart Water Networks (SWNs). Section III reviews customer identity and data anonymity existing techniques that can be implemented in the data aggregation and Blockchain. Section IV, proposes Data aggregation mechanism in details. Section V simulates the customer's identity performance. Section VI concludes the work and state the future work.

II. Blockchain Technology in Smart Water Networks

Blockchain enables peer-to-peer (PTP) transaction in a decentralized network (without intermediates) and all the transaction is conducted in an immutable distributed ledger. Ethereum (Blockchain 2.0) uses the account-based transaction model instead of the unspent transaction output (UTXO) that has been used in Bitcoin. Blockchain technology is based on four aspects; first, consensus, which provides the proof of work (PoW) or proof of stack (PoS) that verifies the action in the network, second, ledger, affords the complete details of the transaction within networks in an immutable way [23]. Third, cryptography, this maintains that all data in the ledger and network, in general, are encrypted, and fourth smart contract which is used to verify and validate the participants of the network [23]. The Conesus is used to be conducted in PoW where users are competing to verify the data to get a minor reward, but this has two disadvantages which are two much energy consumption and centralization. Whenever one of the users verify the process fast it will be included in a mining pool which means the verification will always occur from that pool which transforms the decentralization into centralisation. PoS is suggested in 2011 where only one or few users which are selected based on certain criteria that can validate the work.

There are two types of the Blockchain network can be used; public and private (permissioned). Public Blockchain which can be accessed by anyone in the network. It is still not ready to support scalability as it is considered as time and energy consuming. Private Blockchain requires certain permissions to read and create a new block of the information which can limit the parties that can transact. It can facilitate scalability and privacy for the network along with it has been using with smart devices. For the private blockchains that has permissions on a specific consortium is called Consortium blockchain.

Blockchain can be integrated with Water Networks in four applications;

1. Track the consumption data from smart meters at customer's households to prevent duplication with any other malicious data.
2. Track the data from the hydraulic sensors (i.e., pressure measurements of pipelines) to prevent data tampering of the measurements.
3. Facilitate a secure transfer of data across different sectors and stakeholders.
4. Track water quality and quantity data measurements with customers to provide transparency of the operational process.

Permissioned or consortium blockchains are good candidates for first three applications where Conesus aspect may not be applied which can relax the processing of the data or permissible with consensus can be used to establish high degree of security where not only certain customers can send data but also the data transmitted has to be validated which can limit from data tampering of smart meters attack. Public and permissioned blockchains can be used together for the fourth application where all customers can access the quality and quantity of the water on a real-time basis but they cannot send data and the operation of transmission of the measurements is conducted by only permissioned devices.

Integrating blockchain to the discussed applications can contribute towards many security and trust challenges which are: prevent duplication of water consumption, provide high-security level of identification and authentication for sensing nodes, seamless secure data transfer and avoid data loss from data tampering, high integrity of data, reduce the inefficiencies of the bottleneck problem since there is no intermediary, and provide history of connected devices which can be tracked for troubleshooting purposes. However, these advantages can make a significant impact on Water Distribution System (WDS), but there are some limitation and challenges need to be considered which are: excessive energy, huge computing operations, mining nodes which validates the operations should be selected carefully and scalability of the network increases the complexity. Besides, these limitations, the Smart Water Networks (SWNs) are needed to be upgraded as most of the networks in the industry are based on centralisation manner and the sensing devices including smart meters may not be able to do the computations. Also, some hydraulic sensors underground may not have enough energy for the consensus. Further, there is no universal standard for the communications protocol of the data in where yet some of the common communications protocols can be used.

It is important to mention that the Conesus algorithm should be different than the typical Algorithms due to the nature of the data used in the blockchain, in a matter of consensus, the average consumption or pressure can be used to verify the data yet this section requires further investigation in the future work.

III. Survey of Customer Identity and Data Annymoity Techniques

There are some techniques that can be integrated with blockchain for tracking the smart meters consumption data

to maintain the anonymity of customer's data and identity along with the blockchain operational procedures.

A. Protecting user identity

There are three main techniques that have been discussed in the literature that can be used in SWN to protect user identity [24]. These three techniques are virtual ring [25], anonymisation [26, 27] and pseudonym [28]. In Virtual ring approach, the authentication process has to be approved from the server via a virtual ring as the users send their messages. The server validates their identity using the ring signature without knowing the user's identity [24]. On the other hand, it is difficult to find a malicious user in case one of the users sent a falsified message.

Anonymisation is discussed technique in the literature in preserving user identity [26, 27]. User's credit can be classified into identity information, quasi-identifier (age and gender) and sensitive information. User's credits can be accessed if they have not been anonymized. A Pseudonym is a different name that is assumed instead of the real identity during authentication and bloom filter is usually used in order to match these Pseudonyms with the groups in the database.

In this paper, blockchain is adapted to provide decentralization to avoid such data tampering. A pseudonym is also a well-known technique that protects the user's identity. This method requires signature and zero knowledge proof. A preserving-privacy scheme is proposed in [29] for the smart grid that adopts discrete logarithm to hide the user's identity using signature.

B. Protecting user data

There are three main techniques that have been discussed in the literature that can be used in SWN to protect user data [24]. These three techniques are household battery [30, 31], data aggregation [32, 33] and credential-based technique [34]-[36]. Household battery scheme is used to hide real-time data when consumption goes high whereas battery discharges. Thus, privacy can be protected along with balancing consumption. But this may conflict with the user's economic interest. Data aggregation involves homomorphic encryption and data obfuscation whereas it enables intermediaries to operate on the data without information of plaintext. Two homomorphic encryption methods are often used namely; Paillier encryption and BGN encryption. The obfuscation data is maintained by adding noise into original data. Credential-based is based on blind signature using public key cryptography whereas the user's credentials are approved via control center blindly.

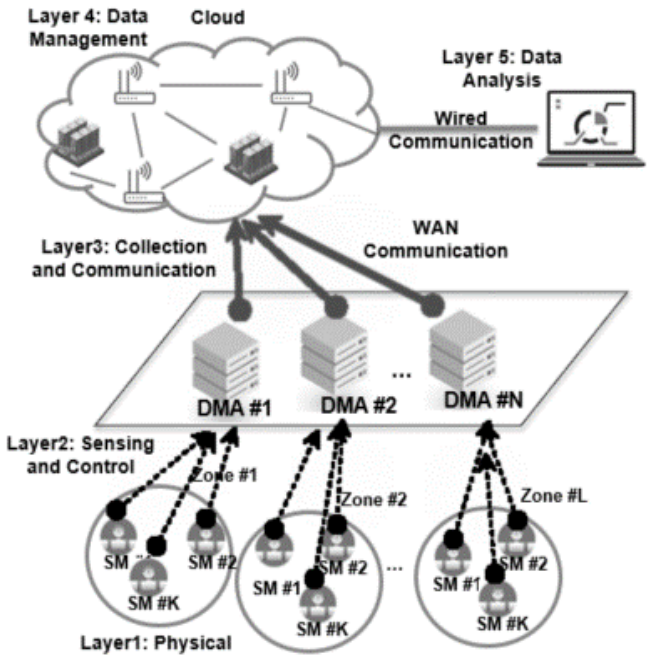

Figure 1. The proposed Network Model.

IV. DATA AGGREGATION MECHANISM

A. Proposed Network Model

The proposed network model consisted of multi-tier network of district area network (DMA) and Wide Area network (WAN) (see Figure 1). Each residential area is covered by DMA for several miles that contain several Smart Meters (SMs) whereas SMs is installed at each households to report real-time water consumption to the utility via DMA. Each subscriber's house is equipped by SM to report the consumption to the utility via local collector called DMA. Each DMA covers L number of zones where each zone contains number of SMs.

All SMs in a certain zone are connected in distributed topology and only one of the SM which are chosen who send all the blocks/packets to the DMA gateway. The data is transmitted from SM to the utility using wireless communications (GSM/GPRS technology). On the other hand, DMA gateways can communicate with the cloud using wired or long-distance -communications. The cloud with the communication of the data analysis center can draw the consumption profile of each household in near real-time data.

When a new SM is created, it first requests the list of trusted nodes (SMs) from root servers which are the central name-servers that is accessed when a user request an information. To ensure integrity and confidentiality, each SM needs to be authenticated with the network (nodes list) to ensure that only legitimate devices are added to the blockchain network. Moreover, every authenticated and encryption process should be done efficiently. This can occur based upon:

- Installed Credentials on SM during setup: There must be a secure procedure in implementing blockchain that could generate these credentials.

- Credentials that can be given by the SM owner: the enrolment process of SM into a server is initialized by the user.

B. *Proposed Data Aggregation Mechanism integrated with blockchain*

The proposed data aggregation mechanism at a certain mining node consisted of six steps: receiving SM data with customer's signature, hash functions, chain block verification, data aggregation, utilities and generating consumption plan, bill and dynamic pricing (see Figure 2).

1. *Encryption, Hash function and Customer's digital signature*

SMs use the public key of the sender ($k_{Sender,\ public}=p\ x\ q$) to send encrypted consumption data, which is then stored in one of the blocks in the blockchain network. Receiver key is then requested by the sender from the ledger for encrypting the consumption. This method will ensure that the only receiver will be able to decrypt the sent consumption data using their private key [23, 37]. When the data is encrypted by a private key, the digital signature is generated by the blockchain which is used to verify the source and authenticity of the data.

A digital signature is a string of text that is extracted from the data and the private key. Thus, it cannot be used for any other process. If the data is changed the digital signature will change. This minimizes the potential attackers that aim to alter the amount of consumption [38]. All the sent data have digital signatures. The procedures of the digital signature are described below [38]:

- The hash of the data is calculated by the sender and then encrypted with the private key. The digital signature is generated based on the data and the public key.
- The digital signature is decrypted using the public key to obtain the hash of the data.
- The resulted hash is compared with the protected hash and it is only valid if they are same. If the digital signature of each sent data is stored into the ledger, the trust of the nodes improves.

2. *Verification of chain block*

After-mentioned the survey of the data and identity anonymity techniques, bloom filter and zero-knowledge proof are good candidates for the data verification of the blockchain. Bloom filter matches that the pseudonyms database of customer's identity with the data in the block and zero-knowledge proof verifies the data consumption without knowing the identity. This verification is conducted by the chosen node which is picked based on the average water consumption and is referred to as mining node.

A Zero-knowledge proof is conducted by making each block answer a complex mathematical problem created using an irreversible cryptographic hash function. In order to solve this mathematical problem, the block has to assign a random number that combined with the previous block -

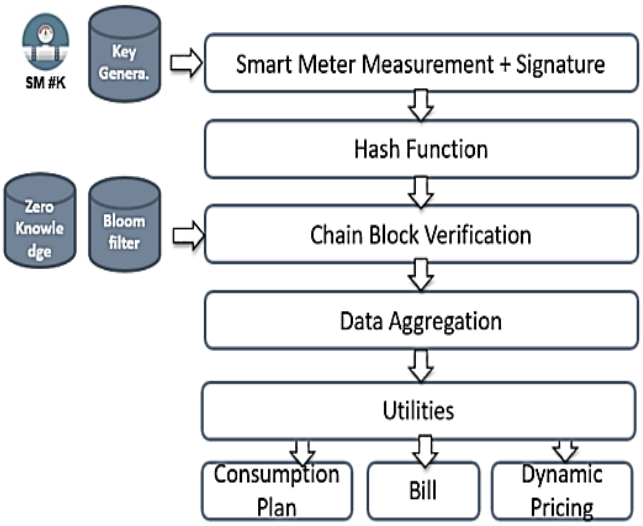

Figure 2. The proposed Data Aggregation Mechanism at the mining node.

content. It may take a year for a typical computer to answer this problem without knowing the previous block content. However, a block is usually solving it in 10 minutes as there is a larger number of computers in the chain. This privilege the node that solved the mathematical problem to place the next block on the chain.

3. *Dispatching, Billing, consumption plan and Dynamic pricing*

After receiving the summation of water consumption from each blockchain in different districts via DMA. The data management and analysis center draw the consumption profile and pattern with respect to the zone. The consumption bill can be calculated and generated at the billing center regarding the dynamic pricing of water tariff about the demands as follows:

$$Bill_{sum} = \sum_{i=1}^{Number\ of\ Days} \sum_{j=1}^{Dynamic\_pricing\_internvals} W_{ij}t_{ij} \quad (1)$$

where W_{ij} and t_{ij} are the water consumption and time period tariff ladder at day i and time interval j. given that there is a three-time period of tariffs in each day.

The financial department in the utility can then calculate the consumption of each customer based on the data in the blockchain blocks in each zone when the billing data comes. A pseudonym is used to hide the real identity of the customers at the same chain. Timely mannered Pseudonym generator block is introduced at each SM where each user randomly changes his water consumption profile with different Pseudonyms. The data to be transmitted can be written as $D_s\ (R_i, TS_i, PSD_i)$, where R_i, TS_i and PSD_i are the user's reporting of SM_i, Timestamp and Pseudonym name which is encrypted by a private key (k).

The consumption plan and Dynamic can be changed based on the quantity of water and consumption patterns in terms of districts. The current water networks that have smart meters are using a fixed water tariff yet there are many publications study the advantages of implementing dynamic pricing scheme [40].

V. Simulation Results and Discussion

The simulation of the proposed data aggregation mechanism focused on the Bloom filter part in contributing to the anonymisation of user identity in a SWN using smart contracts and distributed ledgers in blockchain technology. It is evaluated using the probability of false positive where it can recognize one of the pseudonyms which do not exist. On the other hand, it is guaranteed to have no probability of false negative where it cannot match one of the pseudonyms with an actual existence in the database. The data aggregation mechanism of customer's identity using Bloom filter is simulated with various numbers of users at each DMA. Considering that smart meters can transmit the measurements with maximum of 500 meters as it has been used in the second generation of smart meters (SMETS2) [38]. Hence, we assumed that each DMA will be in charge of communicating with up to 200 smart meters which can represent 25 building with 8 flats at each building.

The impact of the number of users at each DMA on the Probability of False Positive is increasing from the 0 to 0.24 at 1 to 460 (see Figure 3). Since the number of users in the filter increases, the probability of false positive occurring increases as well.

Moreover, the effect of the number of hash function decreasing the false positive at the end till reaches the optimal value of the number of the hash function which is around 7 (see Figure 4). Furthermore, it decreases suddenly at 230 bits in the bloom filter and almost saturates till 1200 bits (see Figure 5). The time complexity is considered with the given system parameters, the time complexity is evaluated using *O(K)* and it is equal 2000. This is much less than other techniques.

VI. Conclusion and Future Work

This paper explores the feasibility and uses cases studies on integrating Blockchain technology with smart water networks. Moreover, the customer's data and identity anonymity techniques that can be integrated with the network are discussed. Furthermore, a data aggregation mechanism of the smart meters in Water Distribution System (WDS) based on distributed ledger and Blockchain technologies is proposed. Further, customer's identity using bloom filter is simulated and optimal parameters of the bloom filter is suggested (7 hash functions, 2000 number of bits of bloom filter for 200 customers at certain DMA).

Integrating Blockchain to the discussed applications can contribute towards many security and trust challenges which are: prevent duplication of hydraulic and water consumption, provide high sensing nodes identification and authentication, seamless secure data transfer and avoid data loss from data tampering, high integrity of data, reduce the inefficiencies of the bottleneck problem since there is no intermediary, and provide history of connected device which can be tracked for troubleshooting purposes. However, these advantages can make a significant impact on Water distribution, but there are some limitation and challenges need to be considered which are: excessive -

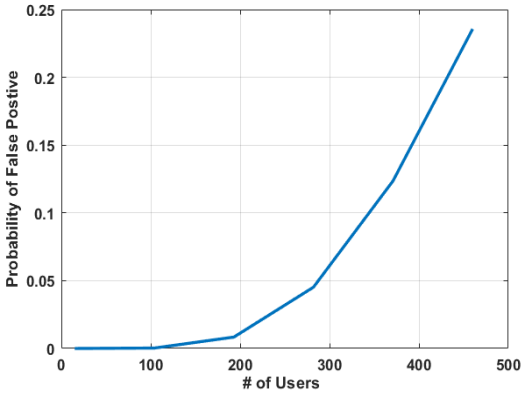

Figure 3. Probability of false positive and number of users at each DMA

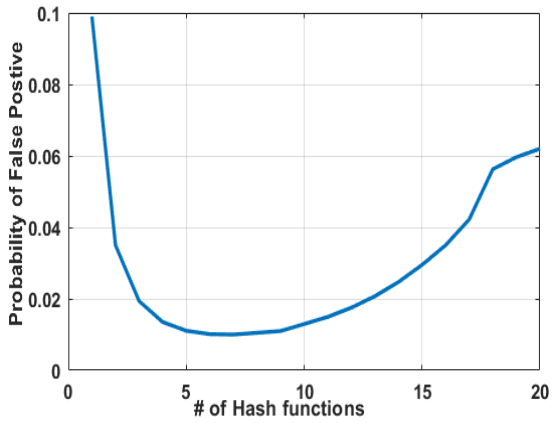

Figure 4. Probability of false positive and number of hash function

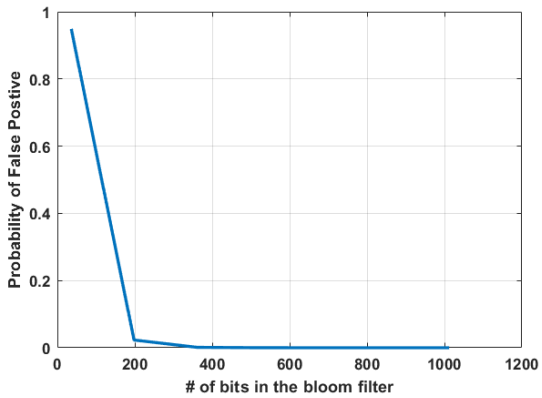

Figure 5. Probability of false positive and number of bits in the bloom

energy, huge computing operations, mining nodes should be selected carefully and scalability of the network increases the complexity. Besides, these limitations, the Smart Water Networks (SWNs) needed to be upgraded as most of the networks in the industry are based on centralisation manner and the sensing devices including smart meters may not be able to do the computations. Also, some hydraulic sensors underground may not have enough energy for the consensus. Further, there is no universal standard for the communications protocol of the data yet some of the common communications protocols can be used.

This work can be extended by consider Blockchain verification block and implement it using one of the open source platforms. Moreover, integrating it Smart Water Networks (SWNs) to track the hydraulic sensors data inside

and outside water plant. Furthermore, implementing it with water quantity and quality sensors to maintain transparency of the operational process. Further, the Conesus algorithms need further investigation because of the nature of the measurement data.

ACKNOWLEDGMENT

This research has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie Training Networks (ITN)-IoT4Win grant agreement No [765921].

REFERENCES

[1] A. Blinder & N. Perlroth, "A cyber-attack Hobbles Atlanta and Security Experts Shudder", 2018.

[2] Verizon's Data Breach Digest, p. 39-42, 2016.

[3] J. H. Germano "Cybersecurity Risk & Responsibility in the water Sector", American Water Works Association (AWWA), 2017.

[4] RiskIQ Evil Internet Minute 2.0 report, 2018.

[5] David Sanger, "Utilities Cautioned About Potential for a Cyberattack After Ukraine's," New York Times, Feb. 29, 2016.

[6] American Water Works Association (AWWA) G30-14 security Practices for operation and management, 2015.

[7] American Water Works Association (AWWA) J100-10 Risk and Resilience Management of Water and Wastewater Systems, 2010.

[8] Emergency Preparedness Practices, ANSI/ AWA G440-17, American Water Works Association (AWWA), 2017.

[9] M. Field, "WannaCry cyber attack cost the NHS £92m as 19,000 appointments canclled",the telegraph, October 2018.

[10] Security Intelligence: ICS-CERT Reports 2015 Infrastructure Attacks, 2015.

[11] The Global Risks Report 2018 13th Edition, 2018.

[12] M. Rovaglio, "IIoT and the Cyber Security Challenge – Part 7 of IIoT and the Oil & Gas Value Chain", 2017.

[13] P. Passeri, "January-September 2018 Cyber Attack Statistics", 2018.

[14] SENSUS Global Survey, [online], 2012.

[15] E. S. Kang, S. J. Pee, J. G. Song and J. W. Jang, "A Blockchain-Based Energy Trading Platform for Smart Homes in a Microgrid," 2018 3rd International Conference on Computer and Communication Systems (ICCCS), Nagoya, pp. 472-476, 2018.

[16] Y. N. Aung and T. Tantidham, "Review of Ethereum: Smart home case study," 2017 2nd International Conference on Information Technology (INCIT), Nakhonpathom, pp. 1-4, 2017.

[17] X. Liang, S. Shetty and D. Tosh, "Exploring the Attack Surfaces in Blockchain Enabled Smart Cities," 2018 IEEE International Smart Cities Conference (ISC2), Kansas City, MO, USA, pp. 1-8, 2018.

[18] J. Vora et al., "BHEEM: A Blockchain-Based Framework for Securing Electronic Health Records," 2018 IEEE Globecom Workshops (GC Wkshps), Abu Dhabi, United Arab Emirates, pp. 1-6, 2018.

[19] S. Chakraborty, S. Aich and H. Kim, "A Secure Healthcare System Design Framework using Blockchain Technology," 2019 21st International Conference on Advanced Communication Technology (ICACT), PyeongChang Kwangwoon_Do, Korea (South), pp. 260-264, 2019.

[20] R. Agrawal et al., "Continuous Security in IoT Using Blockchain," 2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Calgary, AB, pp. 6423-6427, 2018.

[21] B. H. AlDoaies and D. H. Almagwashi, "Exploitation of the Promising Technology: Using Blockchain to Enhance the Security of IoT.," 2018 21st Saudi Computer Society National Computer Conference (NCC), Riyadh, pp. 1-6, 2018.

[22] Z. Guan et al., "Privacy-Preserving and Efficient Aggregation Based on Blockchain for Power Grid Communications in Smart Communities," in IEEE Communications Magazine, vol. 56, no. 7, pp. 82-88, 2018.

[23] M. Singh, A. Singh and S. Kim, "Blockchain: A game changer for securing IoT data," 2018 IEEE 4th World Forum on Internet of Things (WF-IoT), Singapore, pp. 51-55, 2018.

[24] Z. Guan et al., "Privacy-Preserving and Efficient Aggregation Based on Blockchain for Power Grid Communications in Smart Communities," in IEEE Communications Magazine, vol. 56, no. 7, pp. 82-88, 2018.

[25] M. Badra and S. Zeadally, "Design and Performance Analysis of a Virtual Ring Architecture for Smart Grid Privacy," IEEE Trans. Info. Forensics & Security, vol. 9, no. 2, pp. 321–29, 2014.

[26] C. Efthymiou and G. Kalogridis, "Smart Grid Privacy via Anonymization of Smart Metering Data," Proc. 1st IEEE Int'l.Conf. Smart Grid Commun., pp. 238–43, 2010.

[27] Z. Zhou et al., "Software Defined Machine-to-Machine Communication for Smart Energy Management," IEEE Commun. Mag., vol. 55, no. 10, pp. 52–60, 2017.

[28] X. Tan et al., "Pseudonym-Based Privacy-Preserving Scheme for Data Collection in Smart Grid," Int'l. J. Ad Hoc and Ubiquitous Computing, vol. 22, no. 2, pp. 120–27, 2016.

[29] Y. Gong et al., "A Privacy-Preserving Scheme for Incentive-Based Demand Response in the Smart Grid," IEEE Trans. Smart Grid, vol. 7, no. 3, pp. 1304–13, 2015.

[30] Y. Xiao et al., "Stream-Based Cipher Feedback Mode in Wireless Error Channel," IEEE Trans. Wireless Commun., vol. 8, no. 2, pp. 662–66, 2009.

[31] X. Du et al., " A Routing-Driven Elliptic Curve Cryptography Based Key Management Scheme for Heterogeneous Sensor Networks," *007 IEEE International Conference on Communications*, Glasgow, pp. 3407-3412, 2007.

[32] K. Wang et al., "Mobile Big Data Fault-Tolerant Processing for eHealth Networks," IEEE Network, vol. 30, no. 1, pp. 36–42, 2016.

[33] X. Yao et al., "A Lightweight Multicast Authentication Mechanism for Small Scale IoT Applications," IEEE Sensors J., vol. 13, no. 10, pp. 3693–3701, 2013.

[34] X. Du et al., "An Effective Key Management Scheme for Heterogeneous Sensor Networks," Ad Hoc Networks, vol. 5, no. 1, pp 24–34, 2007.

[35] J. Cheung et al., "Credential-Based Privacy-Preserving Power Request Scheme for Smart Grid Network," Proc. IEEE GLOBECOM, pp. 1–5, 2011.

[36] S. Han et al., "PPM-HDA: Privacy-Preserving and Multifunctional Health Data Aggregation with Fault Tolerance for Cloud Assisted WBANs," IEEE Trans. Info. Forensics and Security, vol. 11, no. 9, pp. 1940–55, 2015.

[37] C. Decker and R. Wattenhofer, "A fast and scalable payment network with bitcoin duplex micropayment channels," In Stabilization, Safety, and Security of Distributed Systems, Springer , pp 3–18, 2015.

[38] Michele D'Aliessi, "How Does the blockchain work?, Medium Cryptocurrency, 2016.

[39] Kathryn Porter, "The first SMETS2 smart meters finally arrve but doubts over the programmer remain", 2018.