Keamanan Sistem Kendali Industri dengan Teknologi Blockchain dan Protokol Scuttlebutt

Habiib Tsabit Az Zumar
Institut Teknologi Bandung
habiibaz1404@gmail.com

Abstract— Saat ini industri 4.0 di Indonesia sedang sangat pesat berkembang. Dengan IoT(Internet of Things) sebagai intinya. Pada bidang industri sekarang alat - alat yang digunakan sudah saling terkoneksi satu sama lain ini memungkinkan alat - alat industri bekerja lebih cepat tetapi juga rentan dalam masalah keamanan. Makalah ini menyajikan tentang protokol keamanan dengan menggunakan teknologi *Blockchain* dan *Scuttlebutt Protocol* dengan penggunaan *feed* berantai dari pesan pribadi terenkripsi untuk mendukung integritas dan kerahasiaan komunikasi

Index Terms— IoT, blockchain, scuttlebutt

I. Pendahuluan

Indonesia memasuki era revolusi industri 4.0 dimana pada bidang industri dengan mengintegrasikan teknologi cyber dan teknologi otomatisasi. Pada era industri 4.0 tidak lagi banyak digunakan tenaga manusia karena semua sudah diotomatisasikan. Dengan demikian efektifitas dan efisiensi dapat dimaksimalkan. Dalam penerapannya industri 4.0 mempunyai masalah keamanan yang sangat riskan karena penerapan teknologi informasi yang sangat memungkinkan untuk diretas. Makalah ini dituliskan untuk penyediaan solusi untuk masalah tingkat keamanan pada era revolusi industri 4.0.

Internet of Things (IoT) dan *Blockchain* adalah dua teknologi yang menjadi pelopor perkembangan pada saat ini dan di masa depan. *Blockchain* merupakan teknolog yang memiliki perkembangan yang signifikan. Kedua teknologi ini memiliki perkembangan yang sangat baik. Iot memiliki masalah dalam sekuritas dan *Blockchain* memiliki keunggulan dalam hal keamanan. Penggabungan antara IoT dan *Blockchain* sangatlah menguntungkan bagi industri saat ini.

II. Masalah dan Motivasi

Perkembangan teknologi saat ini sangat menguntungkan bagi pihak industri. Perkembangan pada bidang industri bisa dilihat dari perubahan pada sistem kendali industri atau lebih dikenal dengan ICS (*Industry Control System*) dari elektromekanis menjadi menggunakan teknologi informasi dan komunikasi [1].

ICS ini dirancang untuk data pengawasan dan sistem akuisisi pada perusahaan industri atau biasa disebut SCADA (*Supervisory Control and Data Acquisition*) [2]. SCADA ini bertanggung jawab untuk memantau, mengelola, dan mengendalikan operasi -operasi yang dijalankan dalam kegiatan perindustrian [3].

Kemajuan teknologi mendorong evolusi SCADA pada perusahaan industri. IoT berperan sebagai jembatan antara lingkungan fisik ke dunia maya dari ICS [4]. Dengan terhubungnya ICS ke dunia maya sistem menjadi lebih cepat beroperasi dan lebih mudah berkomunikasi dengan lingkungan satu industri tetapi perkembangan ini tentu mempunyai kekurangan dimana isu keamanan menjadi lebih berbahaya [5].

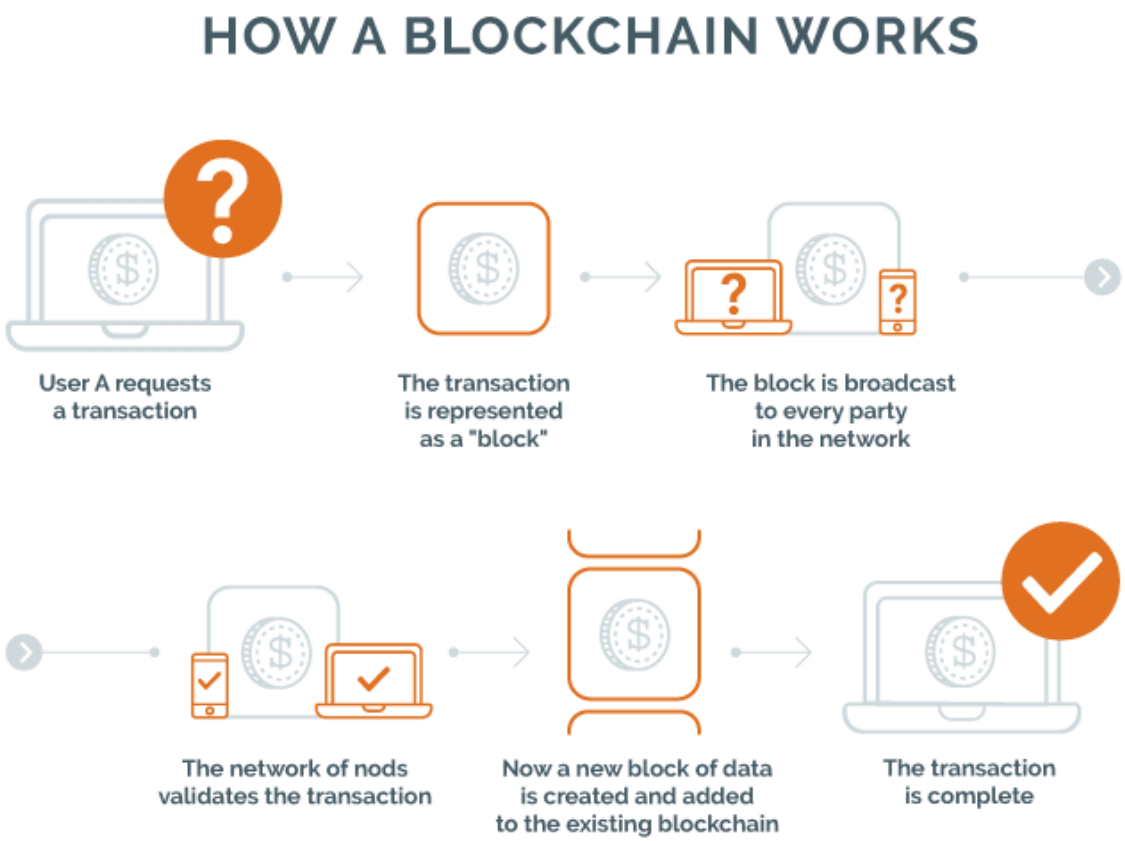
Disaat seluruh perangkat tersambung dengan internet. Ini memudahkan para orang - orang yang tidak bertanggung jawab bisa sangat mudah mencuri informasi. Dengan adanya internet semua pertukaran data akan sangat mudah dilihat dan didapat oleh orang – orang hebat teteapi tidak salah dalam menggunakan ilmunya.

Dalam jurnal - jurnal di internet banyak dibahas tentang pelayanan untuk menyediakan layanan otoritas, integritas, dan kerahasiaan pertukaran informasi pada ICS. Metode - metode yang sering digunakan yaitu enkripsi, *key management system*, dan *software defined network* [6]. Metode -metode di atas seringkali menimbulkan banyak kekurangan diantaranya yaitu tingkat latensi yang tinggi, skalabilitas rendah, dan pemusatan.

Pemusatan data sangat mudah sekali diretas karena data disimpan hanya pada satu pusat yang jika diserang seluruh perangkat akan *down*. Pada kelas Keamanan Informasi di kampus Institut Teknologi Bandung dibahas tentang *Blockchain* yang dapat menjadi solusi bagi tidak amannya pemusatan data. *Blockchain* sendiri merupakan teknologi untuk mendesentralisasikan data yang ada pada ICS, kemudian kriptografi digunakan untuk otentikasi dan integritas data [7].

Blockchain menyediakan data yang terdesentralisasi tidak berpusat. Basis data pada *Blockchain* didistribusikan kepada anggota secara rata dan tidak dapat diubah. *Blockchain*

mempunyai tingkat keamanan yang sangat tinggi karena jika seseorang ingin merubah sesuatu maka dia harus merubah semua data yang dimiliki oleh seluruh anggota. Jika data ada yang tidak cocok dengan satu sama lain maka akan disamakan secepatnya [7].



Gambar 1 : How Blockchain Works (Source: researchgate.net)

Teknologi *Blockchain* ini tetap saja mempunyai kekurangan saat diimplementasikan pada ICS yaitu sistem desentralisasi membutuhkan sumber daya *node* yang luas dan waktu yang substansial untuk memvalidasi dan menyamakan setiap transaksi. Masalah selanjutnya yaitu *Blockchain* tidak bisa merahasiakan sesuatu data hanya pada seseorang anggota, karena sistem *Blockchain* yang mengharuskan untuk persebaran data secara merata.

Pada makalah ini diusulkan komunikasi berbasis teknologi *Blockchain* untuk protokol ICS. *Blockchain* akan menangani masalah keamanan dan penyimpanan data pada sistem. Protokol ini dapat mencapai keuntungan dengan *feed* berantai dari informasi pribadi yang

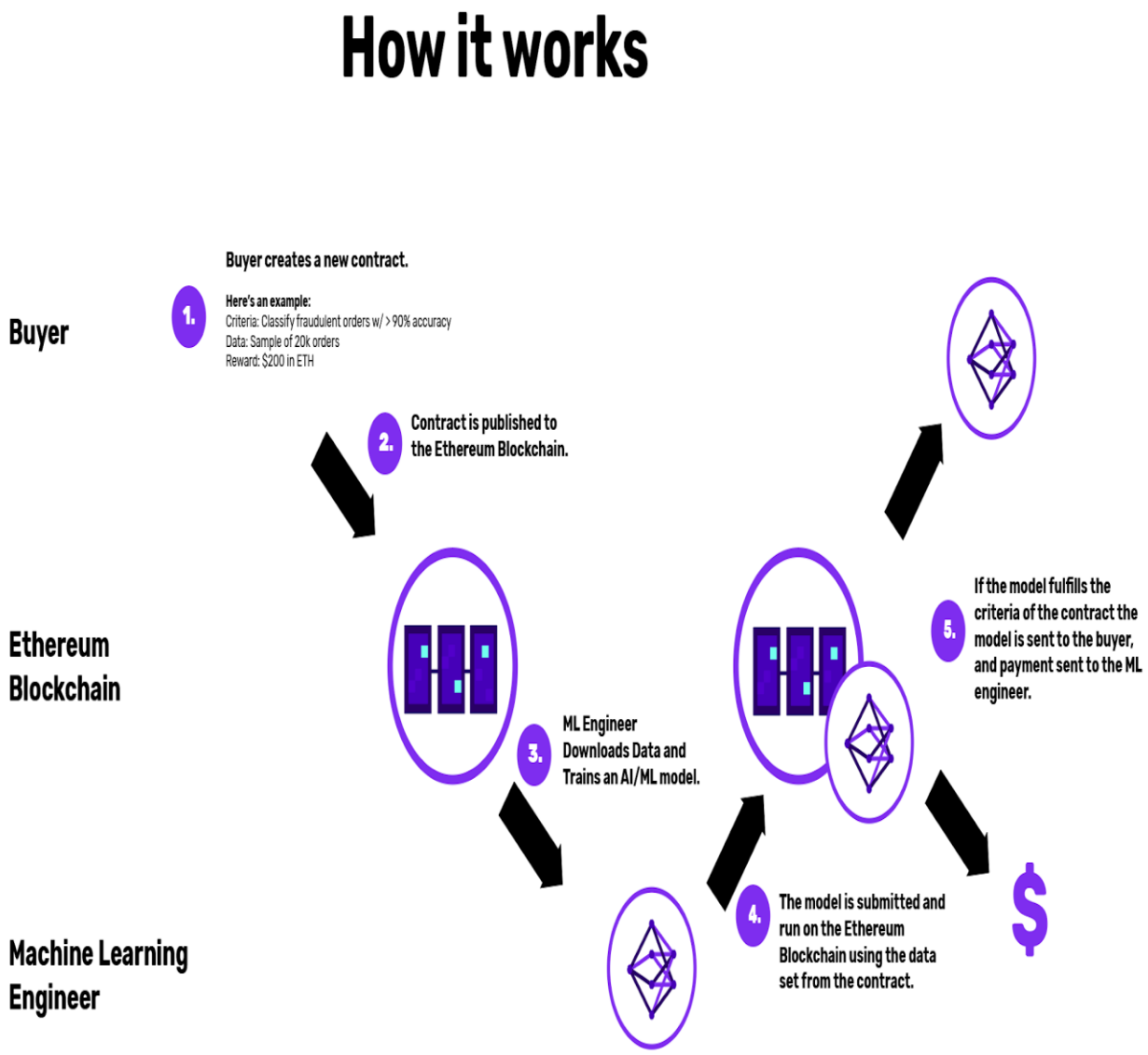
dienkripsi untuk mendukung kerahasiaan dan keamanan informasi. Kemudian akan dibahas tentang strategi pemangkasan untuk menanggulangi masalah penyimpanan perangkat yang luas.

III. Latar Belakang dan Referensi

Model yang diusulkan dalam makalah ini untuk protokol keamanan dibagi menjadi dua bagian. Bagian pertama berfokus pada integritas data. Pada bagian pertama ini sebelum sesuatu prosedur dijalankan, rutin harus memeriksa dan memverifikasi tingkat keaslian data yang akan digunakan. Barulah setelah itu rutinitas selanjutnya adalah menjalankan properti keamanan dengan menggunakan kriptografi.

Bagian kedua berfokus pada aspek komunikasi. Bagian kedua ini menggunakan *key distribution protocol* dengan *symmetric key cryptography* dan *hash* untuk memeriksa keaslian data dari setiap pertukaran pesan yang dilakukan setiap prosedur. Fungsi ini dilakukan oleh simpul khusus bernama *leader group* yang merupakan karya dari Hammi et al [8] dalam tulisannya "Uses the Blockchain Technology for ICS".

Teknologi *Blockchain* juga digunakan pada beberapa platform seperti Ethereum. Ethereum merupakan bahasa pemrograman yang digunakan untuk menyimpan aset uang kripto dengan suatu nilai [8]. Untuk Keamanan pada sistem Ethereum menggunakan otentikasi yang terdesentralisasi. Sistem ini berdasar pada BoT(*Bubble of Trust*). BoT merupakan suatu lingkungan yang terkendali yang dapat bertukar pesan secara aman. Setiap BoT memiliki master yang memegang wewenang untuk memberikan sertifikat pada siapapun yang ingin bergabung pada lingkungan tersebut.



Gambar 2 : Ethereum Blockchain (Source: algorithmia.com)

Pada sistem BoT disoroti beberapa hal tentang waktu rata - rata setiap transaksi pada *Blockchain* yaitu sebesar 14 detik, fase inisiasi memerlukan intervensi vendor, kebutuhan pembayaran pada *cryptocurrency* untuk konfirmasi, dan kurangnya komunikasi antar anggota dalam BoT. IOTA merupakan suatu DLT (*Distributed Ledger Technology)* yang dirancang untuk memenuhi kebutuhan IoT dalam mengatasi dua masalah penting yaitu biaya dan waktu pemrosesan yang tinggi [9].

Distributed Ledger adalah kumpulan dari database yang dimiliki dan diperbaharui secara independen oleh setiap partisipan (biasa disebut *node*) dalam sebuah jaringan yang besar [10].

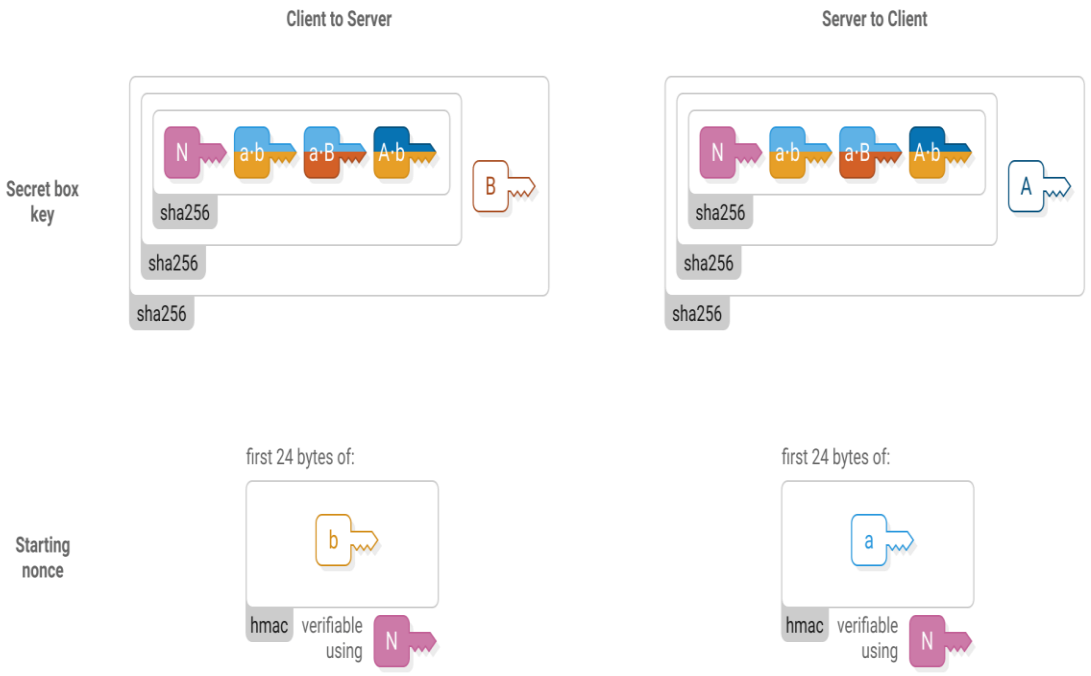
Sistem distribusi ini bersifat unik, catatan tidak diberikan kepada para partisipan oleh sebuah otoritas pusat, tetapi dibuat dan dicatat oleh partisipan masing-masing. Sehingga dengan sistem ini, setiap partisipan di dalam jaringan ikut andil dalam memproses setiap transaksi, membuat beberapa kesimpulan, dan kemudian melakukan voting akan beberapa kesimpulan tersebut sampai sebagian mayoritas setuju dengan kesimpulan yang diambil.

Blockchain tradisional memiliki perbedaan dalam hal bagaimana data terorganisir. IOTA menggunakan DAG (*Direct Acyclic Graph*) yang disebut dengan "The Tangle" untuk menyimpan data transaksi [11]. Pada sistem The Tangle setiap transaksi harus melalui dua tahap validasi melalui *point-of-work* (POW) *algorithm* untuk menyelesaikan kriptografi dengan tingkat kesulitan tinggi menggunakan *hash brute force*.

Brute-force attack masih merupakan salah satu metode peretas kata sandi paling populer. *Brute -force attack* tidak hanya digunakan untuk pemecahan kata sandi. *Brute-force attack* juga dapat digunakan untuk menemukan halaman dan konten tersembunyi dalam aplikasi web. Teknik ini terkadang memakan waktu yang lama, tetapi tingkat keberhasilannya sangat tinggi.

IV. Metode dan Pendekatan

Teknologi *Blockchain* merupakan teknologi yang bisa diandalkan dan tepat untuk mengendalikan dan melacak pertukaran kepemilikan aset. *Blockchain* memiliki tujuan utama untuk menjadi buku besar basis data yang tidak dapat berubah. *Blockchain* tidak dapat dimanfaatkan untuk pertukaran informasi aplikasi. Namun demikian *Blockchain* dapat dipadukan dengan protokol *Scuttlebutt* sebagai protokol pesan untuk menangani masalah keamanan pada ICS.



Gambar 3 : Scuttlebutt Protocol (Source: ssbc.github.io)

Makalah ini akan mengusulkan tentang protokol yang didasari teknologi *Blockchain* dan protokol desentralisasi Secure Scuttlebutt (SSB). SSB adalah protokol basis data untuk *feed* pesan yang tidak dapat dikosongkan [12]. SSB memberikan standar untuk mendefinisikan identitas dan mengelola *feed* pesan.

SSB menggunakan database yang terdistribusi untuk penyimpanan pesan para anggotanya. SSB menampilkan konsep sama seperti sosial media yang berbayar dan dapat diakses oleh publik. Seseorang yang ingin bertukar pesan dan informasi haruslah berlangganan dulu dan bergabung dengan sebuah pub.

Sebuah pub memiliki sosial, ini berfungsi sebagai titik temu bagi para pengguna baru untuk dapat menemukan pengguna lainnya dan menyambut mereka. Para pengguna memiliki seluruh alamat IP anggota yang ada di dalam sosial tadi. Anggota sosial bisa mengakses semua pesan yang diposting oleh anggota lain dan mengirim pesan pribadi mereka juga. Pesan ini dikirim melalui *public-private key pair* seperti pesan yang terenkripsi.

Setelah bergabung dengan pengguna lain seluruh pesan akan di-*upload* dan di-*download* oleh para anggota lain tak terkecuali pesan - pesan pribadi. Anggota baru juga akan mendapat seluruh pesan dan informasi dari pengguna lain. Pendekatan ini merupakan pendekatan yang terdesentralisasi - tidak ada server pusat dan semua komunikasi yang dilakukan para anggota

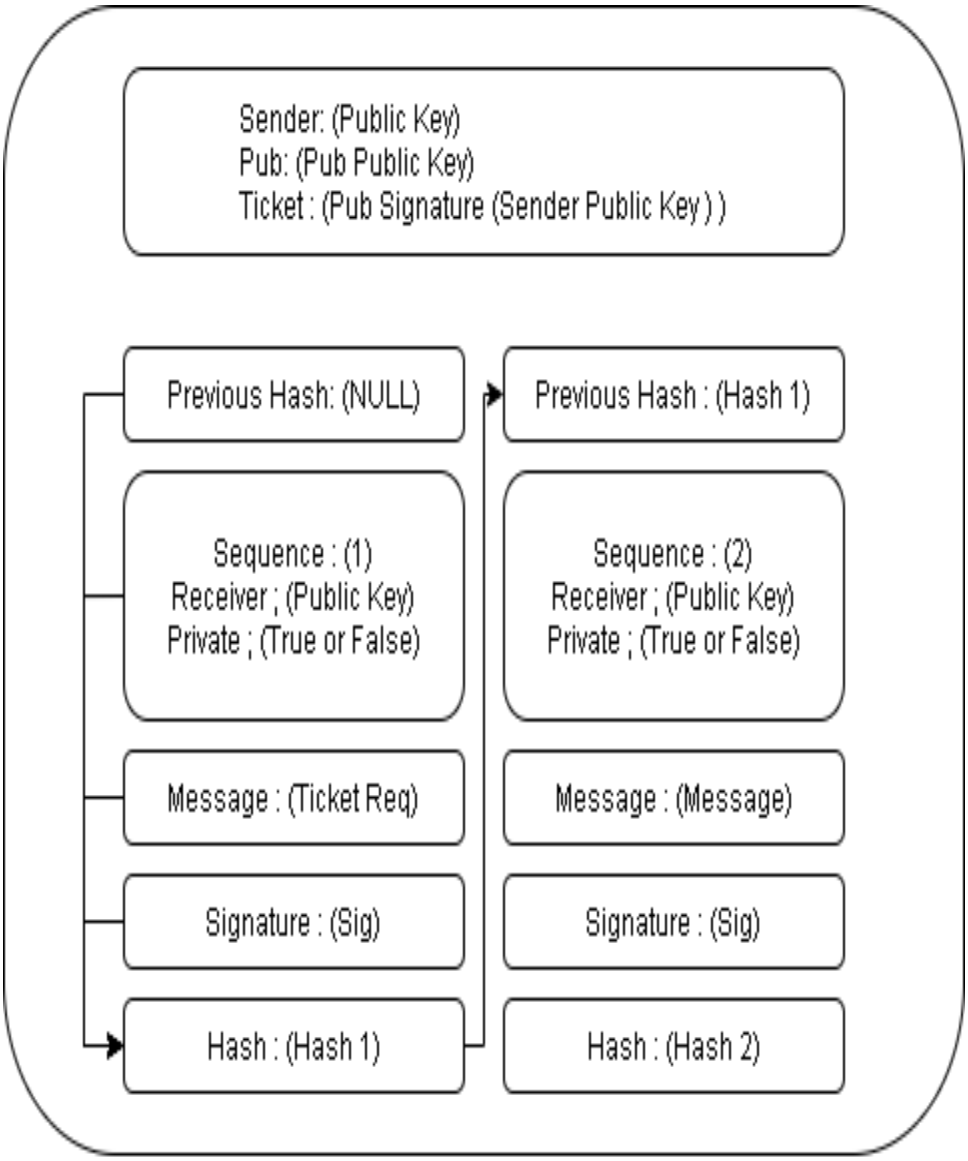
dilakukan P2P. Tujuan dari ini adalah untuk menghindari masalah keamanan dan memberikan skalabilitas ke ICS.

Setiap perangkat pada ICS diharuskan untuk memiliki dua kunci yaitu *private key* dan *public key*. *Public key* berguna untuk mengotentifikasi pesan yang dikeluarkan oleh sebuah *node* dan juga mengenkripsi pesan pribadi. *Public key* menggunakan algoritma asimetris yang mengubah pesan menjadi format yang tidak dapat dibaca. Seseorang yang memiliki public key dapat melakukan enkripsi pesan yang ditujukan kepada penerima tertentu. *Private key* adalah kunci yang digunakan untuk mendekripsi pesan.

Pendekatan pada makalah ini menggabungkan jenis *node* khusus yaitu pub, yang akan bertindak sebagai manajemen registry yang terdistribusi untuk setiap *node* lain di ICS. Pub sama halnya dengan SSB yang menyimpan seluruh alamat IP penggunanya. Untuk menjadi anggota pub sebuah *node* baru membutuhkan undangan. Sebuah pub memiliki daftar undangan yang sebelumnya sudah dibuat dan didistribusikan oleh ICS. Kode undangan yang dibagikan hanya bisa dipakai satu kali, peraturan ini dilakukan untuk menghindari kode - kode dimasukkan ke perangkat ICS dan bisa menjadi ancaman bagi perangkat ICS.

Setelah satu *node* terhubung dengan jaringan, *node* itu harus meminta kepada pihak asosiasi sebuah pub dengan kode undangan secara pribadi dan tidak diungkapkan di dalam jaringan. Jika pub menerima pesan melalui jaringan publik maka akan ditolak. Jika undangan kode valid maka pub akan membuat tiket asosiasi dengan *node public key*, kemudian mengirim tiket ini ke *node*, dan membagikan informasi bahwa ada *node* baru yang masuk kepada *node* terkait lainnya. Dengan metode tersebut *node* terkait yang sudah ada dapat mengotentikasi *node* yang baru bergabung.

Komunikasi antar anggota pub dilakukan secara *peer-to-peer*, untuk melakukan ini seorang anggota harus menyimpan daftar pesan untuk setiap anggota pub lainnya. Hal pertama yang dilakukan adalah mengirim pesan permintaan asosiasi dan ini tidak memerlukan tiket penerbit untuk verifikasi. Lalu pesan yang dikirim hanya dapat dipublikasikan jika pengirim pesan mendapatkan tiketnya. Pesan kemudian akan dienkripsi dengan kode hash. Blok pesan tersebut akan memiliki struktur hash dari blok pesan sebelumnya, kemudian header pesan dengan nomor urut percakapan, isi pesan, dan tanda tangan digital untuk otentikasi pesan. Gambar berikut menunjukan *Feed Structure* dari pesan yang dikirim. Pesan pertama pada *feed* merupakan pesan untuk permintaan ticket.

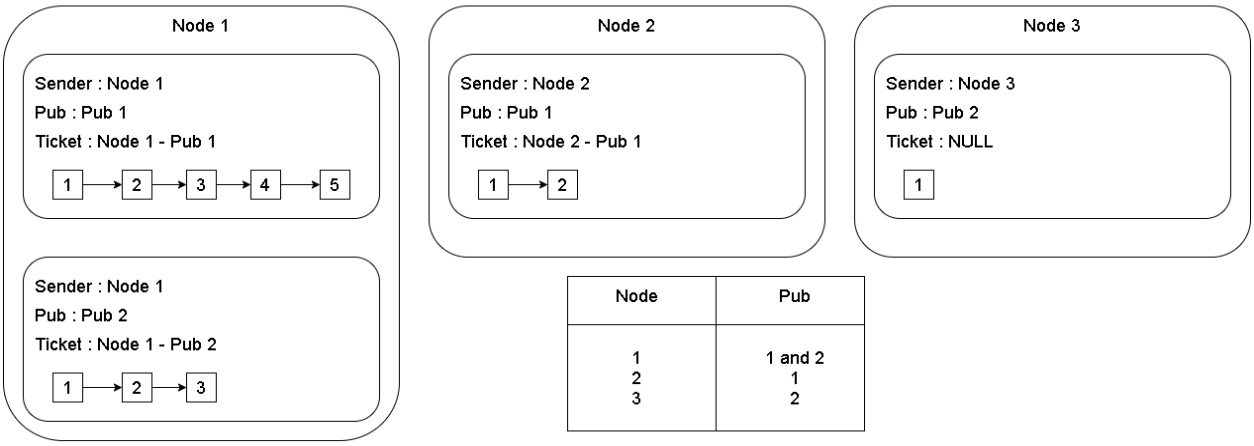


Gambar 4 : Feed Structure (Source: ieee.org [13])

Ketika dua *node* terhubung mereka akan melakukan sinkronisasi dengan memeriksa beberapa hal seperti tiket, tanda tangan, nomor urut blok pesan, dan hash dari blok pesan yang baru. Jika verifikasi berhasil maka blok pesan tersebut akan ditandai sebagai blok pesan yang telah sinkron. Jika tidak maka blok pesan tersebut dan juga blok pesan - pesan selanjutnya akan ditolak. Setelah semua pesan dari semua pub yang terkait telah selesai di sinkronisasi, simpul akan memiliki semua pesan saat ini yang dipertukarkan oleh simpul di pub, yang dikategorikan oleh pub.

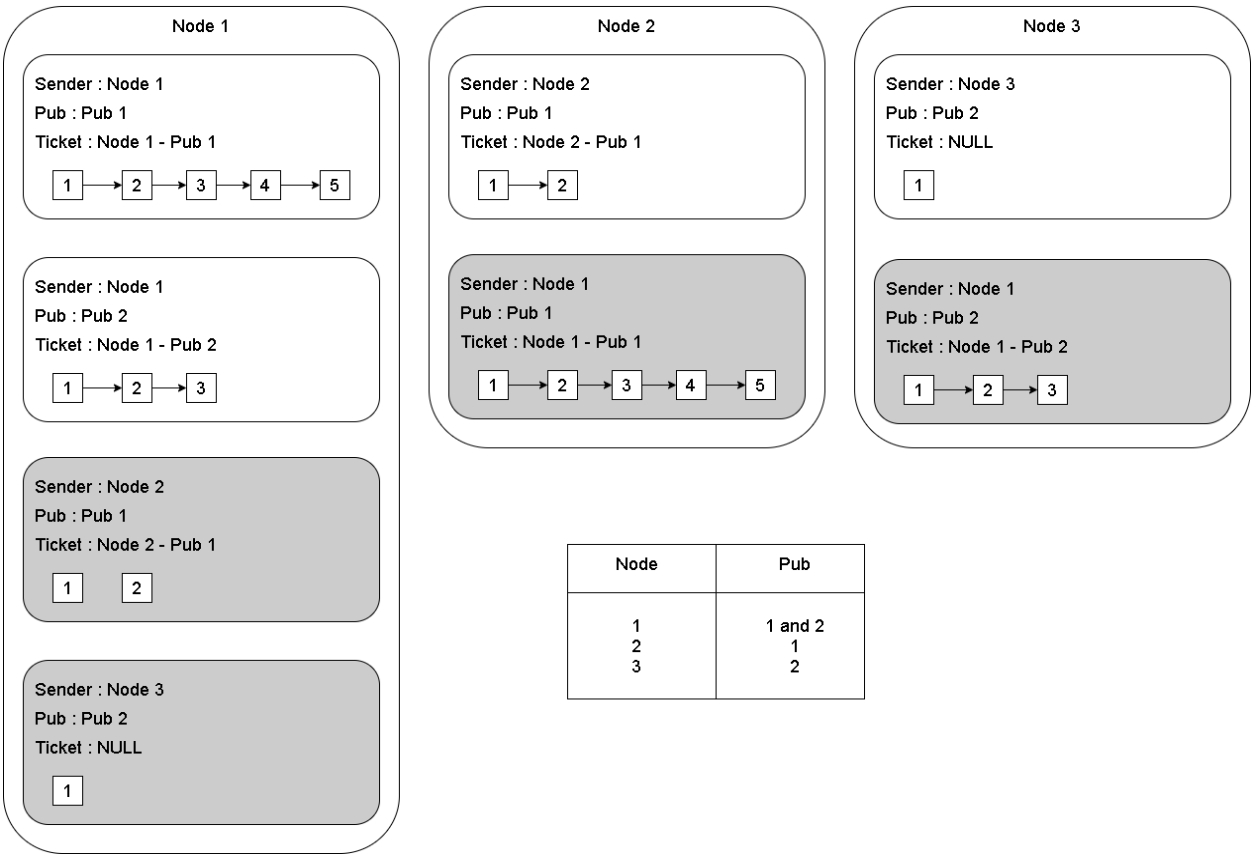
Gambar dibawah akan menggambarkan tiga *node* sebelum dan sesudah sinkronisasi. Semua feed yang telah disinkronisasi akan digambarkan dalam warna abu - abu. Dalam contoh ini pub 1 memiliki dua anggota (Node 1 dan 2) dan pub 2 memiliki dua anggota (Node 1 dan 3). Node 2 dan node 3 tidak dapat saling melihat pesan karena mereka bukanlah satu anggota pub yang sama.

BEFORE



Node	Pub
1 2 3	1 and 2 1 2

AFTER



Node	Pub
1 2 3	1 and 2 1 2

Gambar 5 : Contoh Sinkronisasi (Source: ieee.org [13])

Dalam pengiriman suatu pesan digunakan enkripsi asimetris untuk mengenkripsi data sehingga hanya penerima yang tepat yang dapat men-*decode* pesan. Pengirim menggunakan *public key* penerima untuk mengenkripsi pesan, dan menetapkan tanda pesan menjadi *true* pada *header message*. Jadi hanya penerima yang mempunyai *public key* tersebut yang dapat men-*decode* pesan. Setelah pesan dienkripsi, sebuah *node* harus memperhatikan bahwa penerima harus memeriksa keaslian pesan tersebut. Pengirim harus menandatangani semua pesan yang dikirim menggunakan *private key*. Penerima memverifikasi tanda tangan tersebut dengan menggunakan algoritma verifikasi untuk memeriksa apakah *public* tersebut cocok.

Setiap pesan dimulai dengan hash pesan sebelumnya (atau NULL jika tidak ada pesan sebelumnya) kemudian ditambahkan *header message*. *Header* berisikan nomor urut untuk menghubungkan set pesan dengan benar dan *public key* si penerima. Kemudian terdapat *body massage* yang terenkripsi dan *digital signature*. Seluruh blok pesan dilengkapi dengan kode hash yang mengubah kode string menjadi kode unik yang ukurannya tetap. Ini merupakan fungsi satu arah yang memungkinkan mencari data asli menggunakan kode hash tidak dapat dilakukan. Ini menjamin bahwa pesan belum diubah oleh siapapun ataupun dirusak, pesan masih lengkap, atau tidak ada yang ditambahkan.

Teknologi *Blockchain* mempunyai *timestamp* sebagai metode untuk memastikan keaslian dan urutan suatu transaksi. Pendekatan yang diusulkan menggunakan penomoran yang berurutan, disebabkan oleh dua faktor yaitu perangkat yang terhubung ke internet tetapi *real time clock*(RTC)-nya tidak sinkron dan beberapa perangkat yang mungkin tidak memiliki RTC sama sekali dalam konfigurasinya. Dalam hal ini hal yang diusulkan adalah desentralisasi data dan skalabilitas sistem pendukung struktur pub.

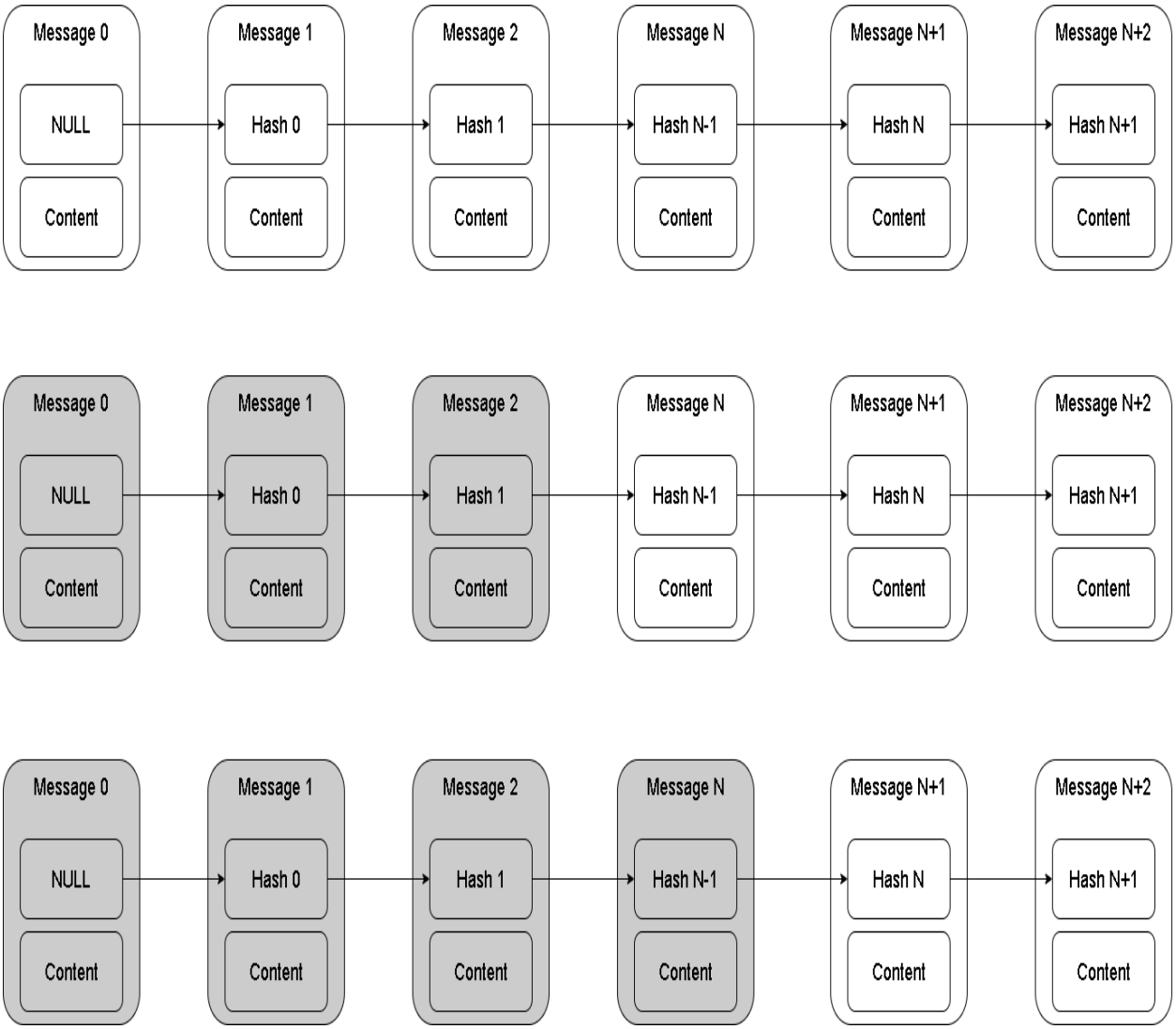
Sistem ini memberikan keamanan dengan cara menggunakan skema tanda tangan yang dilengkapi dengan sertifikat *public key*. Integritas dicapai dengan struktur pesan berantai yang sudah di *hash* dalam suatu *feed*. Pada akhirnya, kerahasiaan data dapat dipenuhi dengan pesan yang sudah terenkripsi menggunakan pasangan *public key* dan *private key*. Namun, *Blockchain* hanya menyediakan database tambahan.

Dalam kendala sumber daya perangkat ICS menggunakan IoT, ini akan menimbulkan dilema seperti yang sudah dijelaskan pada bagian sebelumnya. Tetapi bukan tidak penting juga

suatu perusahaan untuk menyimpan catatan yang panjang dari suatu informasi. Makalah ini mengusulkan pemangkasan untuk penghapusan catatan untuk mempertahankan keaslian dan integritas suatu *feed*, sehingga dapat membuat ruang penyimpanan luang secara berkala.

Prosedur ini memiliki dua parameter yang harus ditetapkan untuk setiap perangkat ICS yaitu ukuran maksimum suatu basis data dan kebijakan tentang penghapusan atau pembuangan data. Selama proses sinkronisasi, jika ukuran basis data yang ditetapkan sudah tercapai, *feed* akan dipangkas dan kemudian pesan terlama dalam *feed* akan dibuang. Setidaknya harus ada minimal satu pesan yang tidak dipangkas agar pesan selanjutnya dapat diverifikasi dengan hash dari pesan pertama yang tersisa. Operator ICS harus memperhatikan pengukuran kapasitas penyimpanan agar tidak terjadi pemangkasan pada pesan yang tidak disebarkan ke seluruh sistem. Ini untuk menghindari keadaan yang tidak konsisten.

Gambar ketiga ini menunjukan contoh pemangkasan di tiga perangkat yang berbeda. Pada makalah ini protokol yang diusulkan juga menghadirkan *node* khusus yang berafiliasi dengan *node* biasa. Meskipun *node* khusus ini bisa dianggap seperti tidak desentralisasi, perannya tidaklah kritis saat terjadi pertukaran pesan. *Node* khusus ini juga tidak berurusan dengan masalah yang ada di *Blockchain* publik, seperti validasi waktu dan algoritma *point-of-work* yang menggunakan daya yang besar untuk mencapai konsensus.



Gambar 6 : Pemangkasan *Feed* di 3 perangkat berbeda (Source: ieee.org [13])

Pendekatan yang diusulkan tetap mempunyai beberapa keterbatasan. Nomor setiap perangkat yang berafiliasi dengan setiap *node* harus dipertimbangkan agar tidak menimbulkan jumlah *feed* yang sangat besar. *Node* ICS yang bertanggung jawab untuk mengontrol dan menganalisis data harus mencatat semua data yang dihasilkan. *Node* tersebut mempunyai komputasi yang tinggi. Masalah lain yang terdapat pada *Blockchain* adalah *private key* yang dapat membuka *cryptographic protection* dari muatan pesan.

V. Hasil dan Kesimpulan

Makalah ini mengusulkan protokol komunikasi untuk jaringan ICS yang mendukung desentralisasi data dan skalabilitas, berkaitan dengan kendala penyimpanan data, dan kerahasiaan data. Solusi yang makalah ini berikan berdasar pada penggunaan teknologi *Blockchain* dan protokol *Secure Scuttlebutt,* kemudian menggabungkan metode *feed* berantai dan pub pada *Blockchain*. Strategi ini memungkinkan untuk mengidentifikasi keaslian perangkat dengan mengimplementasikan penggunaan *digital signature*. Kemudian menggabungkan metode enkripsi-dekripsi menggunakan *public key* dan *private key*. Protokol penyimpanan data juga mengusulkan tentang strategi pemangkasan untuk menangani masalah kapasitas pada penyimpanan data yang terlalu besar.

Pada makalah ini konsep, struktur *feed*, mekanisme pertukaran pesan dan sinkronisasi dirancang dan dicontohkan secara sederhana. Langkah selanjutnya dari makalah ini adalah untuk menyiapkannya pada sistem ICS secara nyata dengan memanfaatkan usulan dari makalah ini. Konsep yang dihadirkan pada makalah ini sangat berguna pada era industri 4.0 saat ini. Kemudahan dalam pertukaran data pada sistem industri didampingi oleh keamanan data dengan metode *Blockchain* merupakan konsep yang harus di terapkan di setiap bidan industri teknologi saat ini.

VI. References

[1] S. McLaughlin, C. Konstantinou, X. Wang, L. Davi, A. Sadeghi, M. Maniatakos and R. Karri, "The Cybersecurity Landscape in Industrial Control Systems," *Proc. IEEE,* vol. 104, no. 5, p. 1039–1057, 2016.

[2] ENISA, "Communication network dependencies for ICS/SCADA Systems," ENISA, 2016.

[3] S. Samtani, S. Yu, H. Zhu, M. Patton, J. Matherly and H. Chen, "Identifying Supervisory Control and Data Acquisition (SCADA) Devices and their Vulnerabilities on the Internet of Things (IoT): A Text Mining Approach," *IEEE Intelligent Systems PP,* vol. PP, no. 99, p. 1–1, 2018.

[4] H. Dai, Z. Zheng and Y. Zhang, "Blockchain for Internet of Things: A Survey," *IEEE Internet of Things Journal,* vol. 6, no. 5, p. 1–1, 2019.

[5] M. Aghashahi, R. Sundararajan, M. Pourahmadi and M. K. Banks, "Water Distribution Systems Analysis Symposium–Battle of the Attack Detection Algorithms (BATADAL)," in *In World Environmental and Water Resources Congress 2017*, Sacramento, California, 2017.

[6] F. A. Alaba, M. Othman, I. A. T. Hashem and F. Alotaibi, "Internet of Things security: A survey," *Journal of Network and Computer Applications,* vol. 88, p. 10 – 28, 2017.

[7] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Future Generation Computer Systems,* vol. 82, p. 395 – 411, 2018.

[8] M. T. Hammi, B. Hammi, P. Bellot and A. Serhrouchni, "Bubbles of Trust: A decentralized blockchain-based authentication system for IoT," *Computers And Security,* vol. 78, p. 126 – 142, 2018.

[9] B. C. Florea, "Blockchain and Internet of Things data provider for smart applications," in *7th Mediterranean Conference on Embedded Computing (MECO)*, US, 2018.

[10] F. Setiawan, "Apa itu Distributed Ledger Technology (DLT)?," Coinvestasi, 20 October 2018. [Online]. Available: https://coinvestasi.com/berita/apa-itu-distributed-ledger-technology-dlt/.

[11] S. Popov, "The Tangle," IOTA, 2018.

[12] Scuttlebutt, "Scuttlebutt Protocol Guide," SSBC, 2019. [Online]. Available: https://ssbc.github.io/.