Pengembangan teknologi *Medical Drone* Serta Analisis Aspek Sekuriti dan Vulnerabilitas Dalam Penggunaannya

Aaron Christopher Tanhar (07211940000055)
Departemen Teknik Komputer
Fakultas Teknologi Elektro dan Informatika Cerdas
Institut Teknologi Sepuluh Nopember
Surabaya, Indonesia 60111
christopher.19072@mhs.its.ac.id

***Abstrak*—Integritas dari sebuah File Digital merupakan salah satu aspek penting dari sekuriti sistem komputer. Terdapat instilah yang dinamakan dengan File Integrity Monitoring (FIM) yang merupakan sebuah proses yang melakukan tindakan validasi dari sebuah File pada Operating System dan software aplikasi menggunakan metode verifikasi antara state atau keadaan yang terkini dengan state yang diketahui atau sebelumnya. Tentu saja hal tersebut penting untuk dilakukan sehingga file-file yang selalu kita transmisikan baik melalui lokal komputer dan melalui nirkabel akan selalu terjamin isinya sehingga tidak korup. Apabila tidak demikian maka mungkin dapat terjadi kerusakan atau pemalsuan data. Maka pada makalah ini saya melakukan riset terhadap metode yang dapat menjamin integritas pada file digital di sistem komputer. Dari segi security, terdapat beberapa penelitian yang juga melibatkan perkara *file integrity*. Penelitian dengan tema secure messaging juga memberikan kita penemuan yang relevan tentang usability dan security dari proses autentikasi pengguna layanan messaging tersebut. Parity Bit atau biasa juga disebut dengan *Check Bit* adalah bentuk sederhana dari *error detecting code*. Terdapat dua varian dari bit paritas, paritas genap dan paritas ganjil. Sebuah checksum merupakan suatu blok data berukuran kecil yang diperoleh dari blok data digital yang lainnya. Sebuah *MD5 message-digest algorithm* adalah hash function yang sering digunakan untuk mengecek integritas pada file. MD5 digest sudah digunakan secara luas pada dunia perangkat lunak untuk memberikan sebuah jaminan dimana file yang ditransmisikan telah tiba dan datanya sama dengan data yang asli. SHA-1 merupakan fungsi *hash cryptographic* yang menerima input lalu akan mengeluarkan output 160-bit (20 byte) nilai hash yang dikenal sebagai *message digest*. SHA-2 merupakan perubahan yang cukup signifikan dibandingkan pendahulunya, SHA-1. SHA-3 adalah subset dari Keccak yang didasari dari pendekatan baru yang dinamakan sponge construction. Sponge construction didasari dari fungsi random atau fungsi permutasi. Sebuah *Cyclic Redundancy Check* adalah *error-detecting code* yang biasa digunakan pada jaringan digital dan storage untuk mendeteksi adanya perubahan yang tidak diinginkan pada data. Komputasi dari CRC diturunkan dari polynomial division, modulo dua.**

***Kata kunci*—*Integrity*, *Security*, Komputer, File, *MD5*, *Checksum*, *SHA*, *Digest*, *CRC*.**

I. Pendahuluan

Drone atau yang biasa juga disebut sebagai pesawat nirawak merupakan pesawat yang tidak memiliki pilot manusia, kru, maupun penumpang yang membuat pesawat ini sepenuhnya independen. Pesawat nirawak yang juga disebut dalam bahasa inggris sebagai *UAV* atau *Unmanned Aerial Vehicle* merupakan sebuah komponen daripada *UAS* atau *Unmanned Aerial System* yang menyertakan kontroller yang berbasis di daratan dan sistem komunikasi dengan *UAV*-nya itu sendiri [1]. Terbangnya pesawat nirawak dapat dikendalikan oleh manusia sebagaimana *remote-piloted aircraft(RPA)*, atau dengan beberapa teknik autonomous, seperti bantuan autopilot, hingga pesawat yang benar-benar autonomous sehingga sama sekali tidak ada intervensi dari manusia [2].

UAV ini awalnya dikembangkan selama abad ke-20 yang diutamakan untuk melakukan misi militer yang dianggap terlalu kotor atau berbahaya untuk dilakukan oleh manusia, dan pada abad ke-21 drone ini sudah menjadi hal krusial yang harus ada pada kemiliteran. Seiring dengan berjalannya waktu dan harga dari drone atau UAV ini menurun maka penggunaannya merambah ke hal-hal yang tidak berbau militer [3][4]. Hal ini termasuk dengan fotografi udara, pengantaran produk atau barang, agrikultur, surveillance, inspeksi infrastruktur, sains[5][6][7][8], penyelundupan[9], dan balapan drone.

Teknologi drone menyediakan keuntungan yang sangat melimpah dan memberi kesempatan yang luas untuk banyak bidang penelitian. Drone dapat melakukan hal-hal seperti halnya surveying, humanitarian work, manajemen resiko bencana, riset dan juga transportasi[10]. Dalam bidang agrikultur, drone dapat melakukan imagery real-time dan sensor data dari lahan pertanian yang luas yang tidak dapat diakses dengan cepat menggunakan kaki ataupun kendaraan[10].

Perkembangan drone berakar dalam dalam sejarah militer. Angkatan Laut AS bersama dengan tim peneliti ulang Inggris di Ordnance College of Woolwich pertama kali bereksperimen dengan torpedo udara dalam upaya memerangi U-boat Jerman dalam Perang Dunia I (Perang Dunia I). Upaya ini memicu penyelidikan terhadap pesawat tanpa pilot. Dari tahun 1922 hingga 1925, Angkatan Laut menguji sistem kontrol radio pada Pesawat N-9. Pada tahun 1924, penerbangan radio-kontrol pertama yang berhasil dilakukan dari lepas landas hingga mendarat [11].

Global Positioning System atau GPS dan juga aplikasi untuk smartphone dan tablet dan meningkatkan kualitas prediksi durasi penerbangan, lebih reliable, dan kemudahan penggunaan serta kemampuan untuk memanfaatkan kamera yang lebih baik dan juga sensor-sensor lain yang dibutuhkan untuk mengaplikasikan drone pada agrikultur dan sumber daya alam[10]. Penggunaan drone menjadi sangat intim dengan beberapa sektor yang dikembangkan dengan ekonomi berkembang. Jika kita kehilangan drone itu maka dapat mengakibatkan implikasi yang berakibat merusak.

Penggunaan drone yang kerap terjadi pada bidang kesehatan atau medis biasanya berupa penyaluran alat-alat paket pertolongan pertama, obat-obatan, penyaluran vaksin, darah, dan kebutuhan kesehatan lainnya yang ditujukan ke daerah terpencil. Hal ini dapat memberikan transportasi test sample yang aman dari penyakit dengan tingkat penularan yang tinggi karena tidak memerlukan manusia untuk langsung terjun di lapangan, dan juga dapat memberikan akses cepat kepada external defibrilator otomatis untuk pasien yang menderita *cardiac arrest* untuk menyelamatkan nyawanya[10] dan selama masa gawat darurat kesehatan. Di era pandemi COVID-19 ini drone dapat mengantar atau menyalurkan *Personal Protective Equipments* (PPE), alat test, vaksin, pengobatan, dan sample dari laboratorium.

Drone dapat membantu untuk melakukan inspeksi social distancing yang mudah secara otomatis[12]. Sebagai teknologi baru, drone dapat menyediakan solusi dari konteks pada keadaan ekstrim darurat, topografi yang sulit, dan infrastruktur transportasi. Pengadopsian drone untuk melakukan pengantaran atau penyaluran benda-benda yang krusial dan obat-obatan yang penting untuk keselamatan kepada seluruh masyarakat dengan keadaan ekonomi apapun dapat mewujudkan kesetaraan kesehatan universal[13]. Keuntungan yang didapatkan dari drone pada sektor transportasi adalah keuntungan logistik dan juga transportasi penumpang[14].

Ekspansi dari penggunaan drone yang pada awalnya hanya digunakan untuk keperluan militer hingga menjadi keperluan sipil juga membuat adanya urgensi untuk melakukan pengembangan teknologi dari drone itu sendiri menjadi lebih baik dan memanfaatkan segala potensi drone yang ada demi masyarakat yang lebih baik. [15, Greenwood (2016)] juga mengatakan bahwasanya untuk menyadari potensi penuh dari sebuah teknologi drone ini, peraturan yang meregulasi penggunaan drone ini sangat diperlukan sembari tetap mengutamakan keamanan masyarakat dan hak-hak privasinya juga. Penyalahgunaan seperti contohnya terorisme, privasi dan penggunaan militer merupakan resiko yang dikhawatirkan terjadi pada penggunaan drone[16].

Meskipun terdapat isu-isu tersebut, [17, Sylvester (2018)] mengatakan bahwa teknologi drone ini dapat memberikan pekerjaan untuk para pemuda yang dapat menggunakan drone untuk menyediakan layanan untuk petani-petani di daerah pedesaan. Berlawanan dengan latar belakang ini, review ini berusaha untuk memperlihatkan pengembangan saat ini daripada penggunaan drone yang ada di sektor agrikultur, bidang kesehatan, dan juga kemiliteran. Untuk menggapai target ini, kita awalnya harus diperlihatkan latar belakang teknikal secara singkat dari drone ini dan pada sektor ini dan juga reviewnya mengambil dari pendekatan analisis SWOT.

Internet of Drones (IoD) meniru akronim dari IoT yang menempatkan "Drones" untuk menggantikan "Things". Maka, IoD ini memiliki beberapa kesamaan dengan IoT atau Internet of Things ini. Gharibi et al. [18] mendefinisikan IoD sebagai arsitektur jaringan kontrol yang berlapis yang dapat membantu untuk mengkoordinasikan drone-drone [19]. Paradigma jaringan IoD ini dapat diaplikasikan dalam operasi Search and Rescue, monitoring angkatan militer, inspeksi industrial, monitoring infrastruktur, sistem pengantaran barang[20], agrikultur [21] [22], mapping supply chain, manajemen bencana [23] [24], dan lain sebagainya. Terdapat ekspektasi kuat yang adalah IoD dapat memiliki peran yang signifikan pada smart city di masa depan [25]. Layanan publik tingkat lanjut sekarang biasanya sekarang dapat mengadakan operasi risiko kritikal alami maupun buatan manusia dengan menggunakan IoD [26] [27].

Akan tetapi, jaringan IoD ini dapat menjadi target dari beberapa ancaman keamanan dan privasi yang berbahaya dan jahat. Baik drone-drone maupun entiti IoD lain mungkin saja dibajak untuk tujuan serangan siber, data breaches, atau pencurian data dengan menggunakan payload. Berdasarkan dari author pada [28], sebuah drone phantom DJI ketika dibajak dapat dijual belikan pada situs ebay dengan harga sebesar 1,000 US dollar. Authornya juga menyatakan bahwa sebuah kamera drone yang digunakan pada industri film dapat dihargai sampai dengan harga 20,000 US dollar, dan sebuah detektor cahaya dan range (LIDAR) sensor dapat diberi harga hingga mencapai 50,000 US dollar. Lebih lagi, ketika sebuah drone yang membawa data yang berharga dibajak, kerugiannya dapat mencapai ribuan US dollar. Kerugian yang jauh lebih besar dapat terjadi ketika drone yang diserang merupakan drone untuk militer. Dampaknya bukan saja hanya membocorkan data berharga atau rahasia ataupun kerusakan fisik dari drone bersangkutan namun juga drone yang dibajak dapat dijadikan sebagai sebuah senjata oleh orang yang membajak [28]. Komunikasi yang terjadi antara drone yang ada di dalam jaringan IoD adalah melalui internet yang tidak aman (umumnya jaringan nirkabel atau wireless maupun WiFi) dan menggunakan sinyal navigasi (contohnya global positioning system (GPS)) [29].

Hal ini dapat mempengaruhi aspek privasi dan keamanan pada drone secara signifikan. Hacker yang tidak bertanggungjawab dapat dengan mudah mengakses konfigurasi dari drone dan membajaknya dengan menggunakan aplikasi open-source untuk membajak drone (contohnya skyjack) dan secara nirkabel mendapatkan kendali dari drone yang menjadi target. Kebanyakan ancaman privasi dan keamanan yang ada pada drone sipil terjadi karena kesalahan pada desainnya. Kebanyakan drone dirancang tanpa perlindungan internet security dan mekanisme autentikasi [30]. Meskipun secara tingkat kesulitan lebih sulit untuk membajak drone pada militer dikarenakan infrastruktur keamanannya yang lebih tinggi apabila dibandingkan dengan drone sipil, seorang hacker yang handal dapat menggunakan teknik yang lebih canggih. Sebuah contoh

dari hal ini adalah CIA RQ-170 Sentinel US spy drone dibajak oleh hacker yang berasal dari Iran pada desember 2011 [31].

Sudah banyak teknik sekuriti, keamanan dan privasi yang dikembangkan oleh peneliti-peneliti untuk mendapatkan jaminan dari keamanan dari jaringan *IoD* atau *Internet of Drones* ini. Teknik yang ditujukan kepada memitigasi atau mencegah masalah yang mempengaruhi lokalisasi keamanan dari drone atau kebutuhab sekuriti yang diasosiasikan dengan jaringan IoD. Serangan lokalisasi error mengganggu kemampuan positioning daripada drone yang terdapat di dalam jaringan IoD sehingga dapat menyebabkan kerusakan yang besar pada performa keseluruhan dari jaringan IoD. Lebih lagi, kebutuhan privasi dan keamanan merupakan tujuan yang menentukan kesanggupan dan fungsi dari jaringan IoD yang didapatkan dari memitigasi ancaman keamanan dan privasi tertentu [32]. Kebutuhan akan keamanan dan privasi dari jaringan IoD ini termasuk dengan integrity, availability, confidentiality, dan privacy preservation.

Malaysia, negara berkembang pesat di Asia, berkomitmen untuk meningkatkan kesehatan ibu melalui berbagai inisiatif strategis seperti pengenalan Penyelidikan Rahasia tentang Kematian Ibu (CEMD) dan pengembangan layanan kesehatan pedesaan [33]. Salah satu parameter penting kesehatan ibu adalah Angka Kematian Ibu (AKI). Keberhasilan luar biasa dicapai pada awalnya, namun, MMR kemudian mendatar dan Malaysia gagal memenuhi target WHO MDG-5 untuk mengurangi AKI sebesar 75% pada tahun 2015. Drone telah digunakan selama bencana di Haiti, Amerika Serikat, Kanada, Karibia, dan Nepal dalam mengirimkan pasokan medis. Itu juga digunakan untuk mengirimkan Automated External Defibrillator (AED) kepada korban serangan jantung di Belanda, dan alat tes HIV di Malawi, Afrika. Contoh-contoh ini menunjukkan penggunaan drone yang meluas sebagai produk medis masa depan. transportasi di seluruh dunia. Meskipun demikian, masih banyak yang harus dilakukan oleh para peneliti untuk memberikan bukti manfaat dan meningkatkan penggunaan teknologi ini secara maksimal termasuk penerapan drone untuk hasil kesehatan ibu.

Terlepas dari minat yang besar, saat ini tidak ada tinjauan sistematis tentang penggunaan drone atau UAV dalam perawatan kesehatan ibu. Oleh karena itu kami berusaha untuk mengisi kesenjangan pengetahuan ini dengan memulai tinjauan sistematis tentang penggunaan drone dalam meningkatkan kesehatan ibu, terutama selama kedaruratan kebidanan seperti PPH. Tujuan dari makalah ini juga adalah untuk menyoroti kerangka potensial penelitian masa depan dalam pengembangan drone khusus kesehatan ibu.

Pembahasan pada paper ini dimulai dengan presentasi mengenai penelitian lain (Bagian II). Terakhir, didapatkan kesimpulan dari penelitian yang telah dilakukan (Bagian VII).

II. Penelitian Terkait

Aspek keamanan dalam drone sipil sudah direview pada [34]. Kemudian, beberapa serangan keamanan pada drone sudah dianalisis pada [35], [36], [37], [38], dan [39]. Metode-metode untuk melakukan deteksi drone dianalisis pada [40], [41], [42], dan [43]. Akan tetapi, keterbatasan utama dari penelitian-penelitian sebelumnya adalah kurangnya analisis yang lebih mendalam dari vulnerabilities dari dronenya itu sendiri serta kurangnya analisis attack life cycle. Terlebih lagi, hanya satu aspek dari keamanan drone yang dianalisis, yakni penyerangan pada drone. Teknik penanggulangan yang saat ini telah ada perlu dianalisis, dan teknik baru perlu diusulkan untuk mengatasi kekurangan dari solusi keamanan pada drone yang ada pada saat ini.

Menurut Yao and Ansari [44], arsitektur IoD pertama dirancang oleh Gharibi et al. [18]. Arsitektur tersebut terdiri dari lima layer konseptual (air space layer, node-to-node layer, end-to-end layer, services layer, dan application layer). Setiap layer dapat mengakses layanan yang sudah diberikan oleh layer dibawah layer tersebut. Lin et al. [45] melakukan penelitian lebih lanjut tentang arsitektur milik gharibi dan menunjukkan kelebihan dan kelemahan dari arsitektur tersebut. Arsitektur tersebut dapat memberikan pencegahan terhadap tabrakan drone saat berada di udara. Kemudian juga dapat memberikan kontrol lebih dimana tempat yang dapat dicapai dan tidak oleh drone. Akan tetapi, terdapat kelemahan yang mana adalah kurangnya penjaluran efektif, kontrol penyumbatan, dan tantangan akan keamanan dan privasi (penyaluran data yang tidak aman). Author mengusulkan solusi yang kira-kira dapat mengatasi permasalahan yang sudah dianalisis yang nantinya akan sesuai dengan arsitektur jaringan IoD.

Terlebih lagi, author di [46] mengusulkan penambahan teknologi blockchain pada layer IoD untuk membuat IoD semakin rahasia, aman, dan *tamperproof*. Qureshi et al. [47] mengusulkan sebuah arsitektur IoD berbasis cloud untuk menyediakan virtualisasi akses pada drone melalui cloud dan mengunggah komputasi yang berat ke cloud dengan batasan resource yang terbatas. Arsitektur ini tersusun atas tiga buah layer. Layer yang pertama adalah drone layer yang merepresentasikan susunan resource ataupun layanan yang diberikan kepada end-users. Pada layer kedua, layer ini disebut sebagai layer layanan cloud. Layer kedua terdiri atas tiga komponen (komponen penyimpanan yang berguna untuk menyimpan data yang didapatkan dari drone, komponen komputasi, dan komponen interface atau antarmuka). Akhirnya, layer ketiga disebut sebagai layer klien. Layer ini memiliki antarmuka dari kedua layer sebelumnya yaitu layer drone dan layer cloud.

Zhang et al. [48] mengusulkan sebuah centralized multi-layered virtual network mapping architecture. Arsitektur tersebut menggunakan virtualisasi dari fungsi jaringan yang menggunakan progres teknologi arsitektur dari IoD milik peneliti-peneliti terdahulu. Fornace et al. [49] mendemonstrasikan penggunaan drone untuk mengkarakterisasi perubahan lahan dan pola deforestasi di Malaysia yang mempengaruhi penyebaran zoonosis daripada parasit dari penyakit malaria. Dalam kasus penelitian lainnya, Barasona et al. [50] menggunakan drone untuk melacak distribusi spasial mamalia besar pembawa tuberkulosis di Spanyol selatan. Baru-baru ini, para peneliti telah menggunakan drone dengan modul analisis asam nukleat untuk mendeteksi Staphylococcus aureus dan virus Ebola [51].

III. Pencarian Literatur

Pencarian literatur secara sistematis dilakukan untuk menilai karya ilmiah yang melibatkan aplikasi medis drone saat ini. Layanan Penemuan EBSCO (Elton B. Stephens Company) digunakan sebagai mesin pencari. Pencarian lanjutan dilakukan untuk mengidentifikasi sumber yang mengandung frasa "drone," "UAV," "kendaraan udara tak berawak," "UAS," dan "sistem udara tak berawak" sebagai istilah subjek. Sumber disusun secara kronologis, dan judulnya disaring untuk relevansi dan dipilih jika dianggap dapat diterapkan. Jenis sumber termasuk majalah, jurnal akademik, artikel berita, publikasi perdagangan, dan sumber daya elektronik. Semua sumber yang diterbitkan dalam bahasa Inggris hingga April 2017 disertakan. Hasil pencarian duplikat tidak diikutkan dalam hasil.

Selanjutnya, dipilih sumber yang membahas penerapan drone di sektor sipil dan dikelompokkan ke dalam 7 kategori besar: pertanian, lingkungan dan konservasi, penegakan hukum dan lalu lintas, pendidikan, konstruksi dan industri, pelayaran komersial, dan obat-obatan. Baik sumber akademik maupun nonakademik diterima. Sumber akademik didefinisikan sebagai sumber yang diterbitkan dalam jurnal ilmiah atau prosiding dari konferensi nasional. Sumber nonakademik dimasukkan dalam upaya untuk menangkap informasi terbaru dalam pelaporan tentang teknologi howdrone yang saat ini digunakan. Sumber yang membahas aplikasi yang sama disertakan. Dari artikel-artikel ini, literatur yang relevan diekstraksi.

Pencarian tambahan digunakan untuk mengidentifikasi sumber yang mengandung istilah "drone" baik dalam istilah subjek atau judul, dan kata "obat" dalam setiap aspek teks. Tujuan dari pencarian ini adalah untuk mengisolasi sumber medis yang mungkin terlewatkan dalam pencarian awal. Paradigma yang digunakan untuk mengolah sumber dari pencarian awal diterapkan, termasuk majalah, jurnal akademik, artikel berita, publikasi perdagangan, dan sumber elektronik dalam bahasa Inggris hingga April 2017. Hasil pencarian disusun secara kronologis. Hasil pencarian duplikat atau artikel yang ditemukan dalam pencarian awal dikecualikan. Sumber yang berkaitan dengan aplikasi medis selanjutnya diindeks ke dalam 3 kategori utama: kesehatan masyarakat/bantuan bencana, telemedicine, dan transportasi medis.

Tema utama dalam kesehatan masyarakat/bantuan bencana meliputi perawatan korban massal, pengumpulan data, penyakit menular, bantuan bencana, dan pengobatan darurat. Dalam kategori telemedicine, deskripsi termasuk drone yang membantu dalam prosedur bedah di lingkungan yang keras yang disimulasikan, termasuk medan perang, dan penggunaan perangkat astelemedis drone dalam pengaturan darurat. Barang perbekalan dan transportasi medis melibatkan beberapa subkategori, antara lain pengiriman barang medis, evakuasi pasien, dan aplikasi komersial untuk infrastruktur.

IV. Pengaplikasian

Penggunaan produk kesehatan dari darah yang cepat, termasuk sel darah merah yang dikemas (PRBC), plasma, dan trombosit, telah terbukti menyelamatkan nyawa pada pasien yang menderita trauma perdarahan [52] [53] [54] [55] [56] [57]. Meskipun banyak rumah sakit yang memiliki akses kritis memiliki produk suplai darah yang tersedia, persediaan terkadang terbatas, dan pasokan trombosit dan plasma biasanya lebih terbatas daripada produk sel darah merah yang ada. Rumah sakit dengan akses kritis didefinisikan sebagai rumah sakit dengan 25 tempat tidur atau kurang yang terletak jaraknya setidaknya 35 mil dari rumah sakit lain melalui jalan utama atau berjarak sekitar 15 mil melalui jalan sekunder [58].

Pusat trauma Tingkat III, meskipun tidak identik dengan rumah sakit dengan akses kritis, seringkali juga terletak di daerah pedesaan dan menyediakan akses penting bagi pasien trauma di daerah tersebut. Sejak awal 1990-an, jumlah pusat trauma tingkat III di Amerika Serikat telah meningkat, tetapi mereka memiliki sumber daya yang terbatas, terutama pusat-pusat di daerah pedesaan [59]. Selain itu, 46,7 juta orang Amerika masih tidak memiliki akses ke pusat trauma tingkat I atau II dalam waktu satu jam dari rumah mereka, dan tambahan 81,4 juta orang Amerika tidak akan, tanpa layanan helikopter, memiliki akses ke pusat trauma dalam waktu satu jam dari rumah [60].

Jadi, bahkan dengan perluasan pusat trauma dalam 2 dekade terakhir, banyak orang Amerika masih memiliki akses terbatas dan berpotensi mendapat manfaat dari tingkat perawatan lokal yang lebih tinggi. Meskipun pusat trauma harus memiliki produk darah segera tersedia, pasokan ini tidak terbatas, dan cadangan yang lebih besar biasanya tidak tersedia. Standar perawatan saat ini merekomendasikan pengangkutan pasien yang membutuhkan transfusi ke rumah sakit yang lebih besar ketika sumber daya, termasuk produk darah, tidak tersedia atau terbatas. Ini seringkali merupakan proses yang mahal dan dapat menunda perawatan awal yang tepat. Upaya telah dilakukan untuk mengatasi masalah ini dengan mengangkut PRBC dan plasma dengan tim transportasi sebelumnya. Meskipun inovatif, perubahan tersebut tidak mengatasi biaya operasi pesawat berawak yang signifikan atau risiko bagi awak penerbangan yang bepergian di daerah terpencil. Selain itu, bencana alam dan insiden korban massal dapat terjadi di lokasi terpencil yang membutuhkan pasokan darah sementara, dan transportasi dapat menjadi penghalang yang signifikan untuk membangun stasiun-stasiun operasi maju ini.

Kemampuan rumah sakit akses kritis untuk mempertahankan inventaris produk darah diperumit oleh banyak faktor, termasuk umur simpan dan biaya. Rumah sakit mungkin memiliki berbagai jenis produk PRBC dan 3 jenis plasma yang tersedia untuk mencegah keterlambatan transfusi darurat. Meskipun masa simpan PRBC (42 hari) dan plasma (1 tahun) relatif lama, produk lain, seperti trombosit (5 hari) dan plasma yang dicairkan (5 hari), dapat terbuang sia-sia ketika permintaan rendah [61]. Rumah sakit akses kritis memiliki persediaan produk darah yang terbatas dibandingkan dengan rumah sakit perawatan tersier yang besar (Tabel 1). Pada pasien dengan perdarahan hebat, transfusi masif (10 unit dalam 24 jam atau 5 unit dalam 60 menit) mungkin diperlukan, yang seringkali dapat dengan cepat menghabiskan suplai darah rumah sakit [62]. Rata-rata pasien trauma yang menjalani transfusi masif membutuhkan rata-rata 22 unit PRBC dan

14 unit trombosit, lebih banyak PRBC daripada stok rumah sakit akses paling kritis [63]. Resusitasi transfusi masif awal juga mencakup plasma, dan rumah sakit akses kritis biasanya memiliki persediaan produk ini yang terbatas.

Bank darah regional yang memasok rumah sakit akses kritis menyimpan cukup darah beku untuk memenuhi permintaan reguler. Selama masa permintaan tinggi atau mungkin hanya untuk 1 pasien dengan perdarahan masif, suplai darah dari rumah sakit dengan akses kritis mungkin akan habis dan memerlukan dukungan intensif dari pusat darah regional [64] [65]. Contohnya adalah selama gempa bumi di Bam, Iran. Peristiwa ini menyoroti inefisiensi dari proses saat ini dimana darah didistribusikan. Meskipun 108.985 unit darah disumbangkan, hanya 23% dari unit ini yang benar-benar didistribusikan ke rumah sakit. Menariknya, hanya 1,3% unit yang dikirim ke lokasi bencana dalam waktu 4 hari [66] . Meskipun banyak faktor yang dapat memperumit tanggap bencana, jelas bahwa distribusi, bukan pasokan, tetap menjadi masalah kritis.

Studi tentang kejadian serupa di Amerika Serikat memperkuat bahwa kekurangan produk darah pada saat bencana alam atau korban massal seringkali tidak menjadi masalah; sebaliknya, logistik distribusi adalah tantangannya. Satu studi menemukan bahwa hanya dalam 4 kasus dalam 25 tahun terakhir lebih dari 100 unit darah telah digunakan dalam 24 sampai 30 jam pertama setelah bencana di Amerika Serikat [64] [66]. Dalam tinjauan bencana baru-baru ini di Amerika Serikat di mana permohonan massal sering mengakibatkan peningkatan donor darah, penundaan yang signifikan ditemukan dalam distribusi sumbangan sensitif waktu ini [67]. Penting untuk dicatat bahwa, karena penyaringan dan pengujian laboratorium, darah biasanya tidak dapat digunakan pada tanggal disumbangkan. Namun demikian, kemampuan untuk secara cepat memindahkan produk darah antar pusat untuk mengatasi kekurangan, tanpa melibatkan manusia dalam proses pengangkutan, akan meningkatkan perawatan pasien dan mengurangi biaya.

Bank darah memiliki sistem pengamanan dan cadangan untuk mencegah kekurangan pada saat terjadi bencana atau peningkatan permintaan. Salah satu metode yang umum digunakan adalah dengan menyimpan sedikit suplai produk darah dan kemudian meminta darah, sesuai kebutuhan, dari bank darah daerah atau rumah sakit daerah. Meskipun sistem ini membantu mengurangi pemborosan produk darah, tingkat pemborosan yang dilaporkan masih berkisar antara 1% hingga 26% [68]. Ketika terjadi peningkatan permintaan, produk darah kemudian dikirim melalui kurir, taksi, ambulans, atau kendaraan polisi [69].

Militer menggunakan metode yang lebih canggih, termasuk truk berpendingin, helikopter yang dipasang di bawahnya dengan beban selempang, dan parasut, untuk menyebarkan darah selama situasi pertempuran. Transportasi darat relatif murah, tetapi risiko terhadap personel tetap ada, dan transportasi dapat terhambat oleh cuaca, kondisi jalan, atau penghematan lingkungan. Transportasi udara konvensional dengan pesawat bersayap tetap atau bersayap putar mahal dan juga membahayakan awak. Meskipun beberapa jaringan trauma secara rutin mengirimkan produk darah dengan kru pengangkut helikopter, ini masih memerlukan pasien untuk kemudian diangkut ke pusat regional, yang menempatkan kru dan pasien pada risiko tambahan. Karena biayanya yang mahal, pesawat tidak secara rutin digunakan untuk mengangkut produk darah sendirian ke pasien.

Oleh karena itu, penggunaan UAV mungkin memiliki aplikasi di bidang kedokteran. Bukan hal yang aneh jika rumah sakit akses kritis memiliki persediaan obat yang terbatas dan variasi obat yang lebih sedikit dibandingkan dengan rumah sakit daerah. Antivenom, misalnya, jarang digunakan, memiliki masa simpan terbatas, dan mahal; Oleh karena itu, tidak praktis untuk menyimpannya di banyak rumah sakit. Akibatnya, pasien harus dipindahkan ke produk atau produk harus dikirim ke pasien, yang dapat menyebabkan penundaan perawatan yang signifikan. UAV dapat memenuhi peran pengirim tanpa risiko untuk mengangkut kru dan tanpa mengharuskan pasien untuk dipindahkan. Demikian pula, perangkat medis seperti perangkat fiksator eksternal, defibrilator otomatis, kasa tempur, dan torniket juga dapat dikirim oleh UAV jika diperlukan. Penggunaan UAV dalam bencana alam telah diusulkan oleh organisasi bantuan bencana. Namun, penggunaan ini juga dapat diperluas ke acara multi-korban di dalam negeri. Dalam keadaan ini, UAV berpotensi digunakan untuk mengangkut pasokan medis darurat ke rumah sakit setempat dan bahkan langsung ke pasien yang terluka di tempat kejadian.

Sistem pengiriman produk darah saat ini di Amerika Serikat bergantung pada kombinasi pemasok regional dan rumah sakit. Rumah sakit akses kritis terkecil di wilayah kami, biasanya 4 hingga 12 tempat tidur, secara rutin menyimpan 2 hingga 6 unit sel darah merah dalam inventarisnya dan tidak ada plasma beku segar atau trombosit. Rumah sakit dengan akses kritis yang lebih besar biasanya membawa 14 hingga 30 unit sel darah merah, 8 unit plasma, dan tidak ada trombosit atau kriopresipitat. Fasilitas ini tidak terlalu sering menggunakan produk darah, sehingga tidak jarang rumah sakit mengirimkan darah yang hampir kadaluarsa (dalam 7-10 hari kadaluarsa) kembali ke rumah sakit yang lebih besar untuk mencegah pemborosan. Rumah sakit berukuran sedang (20-50 tempat tidur) di wilayah kami membawa plasma minimal dan tidak ada trombosit. Hal ini menghasilkan suplai yang sangat terbatas yang mungkin tidak cukup untuk mendukung perdarahan yang signifikan atau protokol transfusi masif. Biasanya, hanya fasilitas regional yang memiliki 50 tempat tidur atau lebih yang memiliki suplai PRBC, plasma, trombosit, dan kriopresipitat yang ekstensif. Menyadari bahwa pedesaan Amerika dilayani oleh institusi medis yang lebih kecil ini, jelas bahwa kualitas perawatan dipengaruhi oleh biaya dan ketepatan waktu pengiriman produk darah, dan bahkan rumah sakit yang lebih besar dapat kehabisan jenis darah tertentu.

V. Public Health dan Medical surveillance

Drone digunakan untuk pengawasan lokasi bencana, area dengan bahaya biologis dan kimia, dan pelacakan lokasi penyebaran penyakit atau pandemi. Telah ditunjukkan bahwa

drone dapat mengumpulkan informasi tentang jumlah pasien yang membutuhkan perawatan dan triase di lingkungan berisiko tinggi. Pada tahun 2013, drone digunakan setelah Topan Haiyan di Filipina untuk memberikan pengawasan udara guna menilai kerusakan awal badai dan memprioritaskan upaya bantuan [70]. Dalam upaya untuk meningkatkan efisiensi tim respons, Layanan Kesehatan Nasional di Inggris telah menyelidiki penggunaan drone untuk menilai cedera yang terkait dengan bahan kimia, biologi, dan nuklir [71].

Teknologi drone telah digunakan untuk mendeteksi bahaya kesehatan, seperti logam berat, aerosol, dan radiasi. Dalam sebuah penelitian dari Italia selatan, drone yang dilengkapi dengan perangkat lunak fotogrametri resolusi tinggi digunakan untuk mengakses dan memprediksi risiko kanker secara akurat dari konsentrasi tembaga tingkat tinggi di area pertanian [72]. Brady et al. [73] mendemonstrasikan kemampuan drone quadrotor dengan platform pengambilan sampel bawaan untuk mengukur aerosol dan melacak level gas secara akurat di medan yang kompleks. Melalui deteksi dini, sistem ini dapat mencegah penyebaran bahaya kesehatan dari patogen. Sejalan dengan itu, teknologi drone juga telah digunakan untuk mendeteksi radionuklida yang khas dalam kecelakaan nuklir dan memetakan radiasi dari tambang uranium [74] [75].

Selain itu, kemampuan drone untuk memperoleh informasi temporal dan spasial resolusi tinggi secara real-time dengan biaya rendah membuatnya layak untuk penelitian epidemiologi. Penggunaan tersebut melibatkan pemantauan deforestasi, perluasan pertanian, dan kegiatan lain yang mengubah habitat alami dan komunitas ekologis. Fornace et al. [49] mendemonstrasikan penggunaan drone untuk mengkarakterisasi perubahan lahan dan pola deforestasi di Malaysia yang mempengaruhi penyebaran zoonosis daripada parasit dari penyakit malaria. Dalam kasus penelitian lainnya, Barasona et al. [50] menggunakan drone untuk melacak distribusi spasial mamalia besar pembawa tuberkulosis di Spanyol selatan. Baru-baru ini, para peneliti telah menggunakan drone dengan modul analisis asam nukleat untuk mendeteksi Staphylococcus aureus dan virus Ebola [51].

Malaysia, negara berkembang pesat di Asia, berkomitmen untuk meningkatkan kesehatan ibu melalui berbagai inisiatif strategis seperti pengenalan Penyelidikan Rahasia tentang Kematian Ibu (CEMD) dan pengembangan layanan kesehatan pedesaan [33]. Salah satu parameter penting kesehatan ibu adalah Angka Kematian Ibu (AKI). Keberhasilan luar biasa dicapai pada awalnya, namun, MMR kemudian mendatar dan Malaysia gagal memenuhi target WHO MDG-5 untuk mengurangi AKI sebesar 75% pada tahun 2015. Drone telah digunakan selama bencana di Haiti, Amerika Serikat, Kanada, Karibia, dan Nepal dalam mengirimkan pasokan medis. Itu juga digunakan untuk mengirimkan Automated External Defibrillator (AED) kepada korban serangan jantung di Belanda, dan alat tes HIV di Malawi, Afrika. Contoh-contoh ini menunjukkan penggunaan drone yang meluas sebagai produk medis masa depan. transportasi di seluruh dunia. Meskipun demikian, masih banyak yang harus dilakukan oleh para peneliti untuk memberikan bukti manfaat dan meningkatkan penggunaan teknologi ini secara maksimal termasuk penerapan drone untuk hasil kesehatan ibu.

Salah satu penggunaan drone yang paling menjanjikan adalah di bidang telemedicine yang sedang berkembang—diagnosis jarak jauh dan perawatan pasien melalui teknologi telekomunikasi [76]. Kata kunci dalam definisi telemedicine adalah telekomunikasi. Sayangnya, komunikasi yang diperlukan untuk misi telemedicine ke lingkungan terpencil, bantuan bencana, atau pertempuran tidak dapat bergantung pada jaringan komersial. Ide pendirian Infrastruktur Telekomunikasi Instan (ITI) menggunakan drone dibahas oleh penulis senior (JCR) di Athena, Yunani, pada tahun 1998 di Program Tele-medicine Pusat Ruang Angkasa Komersial Yale /NASA Gambar 4. Presentasi platform drone showcaseda yang berkonsentrasi pada penyediaan komunikasi untuk melakukan evaluasi pra dan pasca operasi pasien dan telementoring prosedur bedah tertentu di daerah terpencil. Telementoring adalah pemberian bimbingan jarak jauh oleh ahli bedah berpengalaman ataupun proseduralis ke rekan yang kurang berpengalaman, dengan prosedur yang muncul menggunakan komputer dan telekomunikasi [77]. Dengan menggunakan konsep ITI ini, Harnett et al. [78] mendemonstrasikan bagaimana drone dapat digunakan untuk membangun jaringan komunikasi nirkabel antara ahli bedah dan robot untuk melakukan telesurgery—kinerja prosedur bedah menggunakan robot, dengan operator berada jauh dari lokasi pasien. Dalam penelitian tersebut, ahli bedah dan robot ditempatkan di tenda dengan jarak 100 meter. Ahli bedah berhasil mengoperasikan lengan robotik untuk melakukan latihan simulasi manuver bedah. Baru-baru ini, para peneliti telah memperluas penyelidikan ke skenario perawatan yang tidak terlalu ekstrem. William CareyUniversity College of Osteopathic Medicine menguji drone telemedis untuk mengirimkan pasokan medis dan paket komunikasi untuk skenario klinis darurat guna membantu memberikan perawatan [71].

VI. Keamanan dan Serangan pada Jaringan IoD

Bagian ini membahas ancaman fisik yang mempengaruhi keamanan drone, yang merupakan entitas terpenting dari jaringan internet of drone (IoD). Masalah keselamatan ini secara signifikan mempengaruhi pencapaian misi yang ditargetkan. Selain itu juga dihadirkan model ancaman, model keamanan dan privasi, serta serangan pada jaringan IoD.

A. Isu Keamanan pada Internet of Drones

Terlepas dari masalah keamanan dan privasi jaringan IoD, drone, yang merupakan komponen utama jaringan IoD, rentan terhadap ancaman fisik yang memengaruhi keselamatan mereka, yang menghambat pencapaian misi. Ancaman fisik yang paling parah adalah pencurian dan perusakan. Karena drone dioperasikan di udara/perairan terbuka, mereka rentan terhadap pencurian, pembajakan fisik, dan penghancuran menggunakan senjata dan riak anti-drone [79]. Maldrone, virus perangkat lunak, digunakan oleh peretas untuk menyabotase dan mengganggu komunikasi tautan data dan memaksa drone sipil untuk mendarat secara instant [80].

Skenario lain adalah menggunakan drone musuh untuk bertindak sebagai predator drone. Drone jahat ini dibangun dengan jaring ikan yang secara fisik menangkap drone target. Ancaman fisik drone paling berbahaya kedua adalah kondisi cuaca dan tantangan sipil. Kondisi cuaca yang buruk, termasuk suhu rendah atau tinggi, turbulensi, badai petir, dan hujan yang membekukan, dapat menyebabkan kecelakaan drone. Drone ukuran kecil lebih rentan terhadap ancaman ini dibandingkan dengan drone ukuran lebih besar. Elemen sipil yang mempengaruhi navigasi drone termasuk gedung tinggi, pohon besar, dan kabel listrik. Ancaman fisik ketiga untuk drone adalah tabrakan antara drone ramah yang sedang bergerak. Ini terjadi ketika drone berbeda yang tergabung dalam jaringan IoD yang sama secara tidak sengaja menyerang satu sama lain karena kesalahan mekanisme sense-and-avoid bawaan.

Seperti yang dibahas di bagian ini, ukuran drone memiliki efek serius pada keamanannya. Drone yang lebih kecil lebih rentan terhadap ancaman keamanan dibandingkan dengan drone yang lebih besar. Ini karena drone yang lebih kecil tidak dapat mengakomodasi mekanisme keamanan yang efisien karena fitur kendala sumber dayanya. Oleh karena itu, penelitian masa depan diperlukan pada pengembangan mekanisme keamanan ringan yang cocok untuk drone yang lebih kecil.

B. Model ancaman pada jaringan Internet of Drones

Model ancaman adalah prosedur di mana potensi kerentanan atau serangan diidentifikasi dan mitigasinya dapat ditentukan. Model menggambarkan sifat penyerang, vektor serangan, area jaringan yang mudah diserang, dan tindakan pengendalian yang harus diambil. Singkatnya, pemodelan ancaman adalah prosedur untuk menentukan semua potensi ancaman yang dapat membahayakan jaringan atau sistem [71]. Beberapa metode pemodelan ancaman telah dikembangkan selama bertahun-tahun. Namun, tidak semuanya cukup komprehensif untuk jaringan cyber-fisik yang kompleks seperti internet drone (IoD). Oleh karena itu, model ancaman untuk jaringan IoD harus lebih kuat dengan gambaran yang jelas tentang potensi ancaman. Ada banyak model ancaman yang digunakan pada jaringan IoD oleh berbagai peneliti. Model ancaman utama dan paling dapat diterima untuk jaringan IoD diberikan di bagian ini.

Model ancaman Dolev Yao diusulkan oleh Dolev and Yao [81]. Model ini diterima secara luas untuk protokol kriptografi. Model ancaman CK diusulkan oleh Canetti and Krawczyk [82]. Model ancaman memiliki semua karakteristik model Dolev Yao. Selain itu, terlepas dari semua hak istimewa yang diberikan kepada musuh dalam model Dolev Yao, musuh model CK dapat mengkompromikan parameter rahasia termasuk kunci pribadi yang disimpan dalam memori entitas jaringan asli dengan menggunakan serangan analisis daya. Model ancaman pohon serangan menggunakan metodologi pohon serangan pada sistem dan jaringan fisik-cyber [83]. Model ancaman pohon serangan pertama kali diusulkan oleh Schneier [84]. Pohon serangan adalah ilustrasi diagram serangan dalam bentuk pohon. Akar pohon menandakan tujuan serangan, dan daun melambangkan cara untuk mencapai tujuan. Tujuan yang berbeda direpresentasikan dengan pohon terpisah yang menghasilkan model analisis ancaman yang melibatkan sekumpulan pohon. Pemodelan ancaman pohon serangan cukup mudah digunakan. Namun, ini membutuhkan pengetahuan yang luas tentang jaringan atau sistem yang sesuai dan masalah keamanannya.

C. Model keamanan dan privasi pada jaringan Internet of Drones

Model keamanan dan privasi adalah desain arsitektur dan prosedur yang mewakili entitas jaringan dan hubungannya dalam membangun keamanan dan privasi. Model yang ditujukan untuk menetapkan persyaratan keamanan dan privasi jaringan atau sistem yang sedang dipertimbangkan. Banyak model keamanan dan privasi telah dipertimbangkan pada jaringan IoD oleh para peneliti.

Model ini terdiri dari tiga entitas utama: Pusat otoritas tepercaya (TAC), drone terbang, dan stasiun kontrol darat (GCS) [85] [32] [86]. TAC dipercaya sepenuhnya oleh semua entitas jaringan internet of drones (IoD). Ini mendaftarkan semua entitas IoD lainnya dan menghasilkan pasangan kunci mereka. Drone terbang adalah komponen kunci dari jaringan IoD yang terletak di berbagai zona terbangnya. Kontrol keseluruhan drone dilakukan oleh GCS. Setelah pendaftaran entitas jaringan dan pembuatan kunci oleh TAC berhasil, entitas terdaftar yang ingin berkomunikasi akan menghasilkan dan menyetujui kunci sesi bersama. Kunci sesi bersama akan digunakan untuk memastikan komunikasi yang aman dan autentik.

Model keamanan dan privasi berbasis blockchain yang khas untuk jaringan IoD terdiri dari tiga lapisan: Lapisan pengguna, lapisan infrastruktur, dan lapisan IoD [87]. Di lapisan pengguna, interaksi antara dua pengguna dan interaksi antara pengguna dan drone ditentukan. Jumlah pengguna dan drone digabungkan untuk membuat cluster blockchain dengan drone sebagai pengontrol utama. Setiap cluster digunakan untuk mengontrol dan mengkoordinasikan perilaku drone. Blockchain memberikan keamanan dan privasi ke jaringan. Lapisan infrastruktur menentukan konektivitas dan kontrol pengguna dan drone melalui stasiun kontrol darat (atau stasiun pangkalan). Terakhir, lapisan IoD menentukan komunikasi antara pengguna dan drone untuk pertukaran data yang efisien dan aman menggunakan teknologi blockchain. Mereka berkomunikasi melalui internet dan informasi terbaru mereka disimpan di blockchain.

Model keamanan dan privasi otentikasi pengguna yang khas untuk jaringan IoD terdiri dari drone terbang, server (ruang kontrol), dan pengguna [88]. Drone terbang mengirim data terus menerus ke server. Otentikasi jarak jauh antara drone terbang dan pengguna dibuat melalui server. Pengguna dan drone terbang berbagi kunci sesi yang sama dan memulai komunikasi setelah otentikasi bersama. Oleh karena itu, setiap pengguna di jaringan IoD dapat memperoleh informasi secara aman dari drone terbang.

Dalam model keamanan dan privasi jenis ini, beberapa entitas jaringan IoD dengan fitur yang sama atau bahkan berbeda bergabung membentuk grup dalam melakukan otentikasi [89].

Ini secara signifikan mengurangi overhead komputasi dibandingkan dengan otentikasi individu. Manajer grup, dengan sumber daya yang lebih baik dibandingkan dengan semua anggota grup menghasilkan semua parameter yang diperlukan untuk proses otentikasi grup. Anggota grup dapat berupa stasiun kontrol darat (base station), perangkat komputasi tepi seluler (MEC), atau otoritas tepercaya.

D. Serangan pada jaringan Internet of Drones

Klasifikasi serangan di internet drone (IoD) diberikan di bagian ini. Lokalisasi atau estimasi posisi adalah kebutuhan penting dari setiap sistem cyber-fisik seperti IoD [90]. Oleh karena itu, serangan yang menyebabkan kesalahan lokalisasi entitas IoD sangat merusak. Oleh karena itu, dalam pekerjaan tinjauan ini, semua serangan jaringan IoD diklasifikasikan hanya ke dalam dua kategori utama. Semua serangan yang menghalangi estimasi posisi aman drone dikategorikan dalam serangan kesalahan lokalisasi, dan serangan lainnya dikategorikan dalam serangan terhadap persyaratan keamanan dan privasi. Serangan terhadap persyaratan keamanan dan privasi disubkategorikan menjadi serangan terhadap integritas, ketersediaan, keaslian, kerahasiaan, dan privasi.

1) Privasi: Privasi merupakan perhatian penting untuk keamanan berorientasi data di IoD. Data dikumpulkan 5 Internet Drone Choudhary dkk. dan diproses melalui IoD dan pemrosesan data meningkatkan kemungkinan ancaman dan kerentanan. Penyerang menargetkan IoD untuk mendapatkan informasi sensitif melalui berbagai pendekatan. Serangan berikut mempengaruhi privasi IoD.

a) Analisis lalu lintas: Analisis lalu lintas dilakukan untuk memeriksa lalu lintas IoD untuk mendapatkan beberapa informasi yang berguna dari perangkat dan jaringan IoD. Lalu lintas berisi paket yang dibagikan antara IoD dan sistem kontrol tanah. Forensik paket dalam lalu lintas mengungkapkan informasi sensitif. Paket termasuk informasi seperti lokasi, IoD yang terhubung dengan sensor, dan menangkap data dari sensor

b) Interception: Dalam intersepsi, penyusup melibatkan seseorang yang secara rutin memonitor jaringan lalu lintas. Sangat sulit untuk menemukan penyusup seperti itu yang secara pasif memantau jaringan. Dalam misi kritis, IoD berisi informasi sensitif; oleh karena itu pelacakan dan pemantauan dari IoD bisa berbahaya bagi lembaga yang bertanggung jawab untuk misi tersebut.

c) Pengambilan data dan forensik: Melalui analisis lalu lintas, sejumlah besar data dapat dikumpulkan dari IoD. Bahkan jika data terenkripsi tidak mengungkapkan informasi yang berguna, forensik data membantu untuk mendapatkan informasi sensitif dari data yang dikumpulkan. Dengan demikian, diinginkan untuk merumuskan solusi untuk mencegah pelanggaran informasi jika mekanisme berbasis forensik diterapkan untuk menyerang IoD.

2) Integrity: Integritas mendefinisikan bahwa data dalam IoD harus konsisten, akurat, dan tepercaya. Itu transmisi tidak boleh diubah dalam komunikasi oleh pengguna atau penyerang yang tidak sah [91]. Beberapa mekanisme yang umum digunakan untuk perlindungan integritas data adalah fungsi hash, checksum dll. Integritas IoD dipengaruhi oleh serangan berikut:

a) Substitusi atau pengubahan informasi: Perubahan adalah konsep penambahan false atau informasi yang salah dalam komunikasi dan mengubah arti asli data. Berbagai bentuk perubahan meliputi modifikasi, fabrikasi, substitusi, dan injeksi data yang memodifikasi data yang digunakan dalam komunikasi IoD. Perubahan data sesat pengguna dengan informasi palsu.

b) Modifikasi kontrol akses: Kontrol akses adalah aturan dan kebijakan yang mengatur bagaimana perangkat lain di IoD berkomunikasi dan bagaimana pengguna mengakses data. Kontrol akses adalah pikiran dari tubuh yang memberikan instruksi kepada IoD. Jika penyerang memperoleh kontrol akses, maka penyerang dapat mengubah semua izin, hak istimewa, dan otorisasi, yang mungkin mengakibatkan kerugian yang besar.

c) Serangan Man-in-the-Middle: Serangan Man-in-the-Middle memungkinkan penyerang untuk menangkap data pada komunikasi antara IoD dan sensor. Titik Akses Rogue digunakan untuk memiliki titik akses nirkabel dan menipu perangkat terdekat untuk bergabung dengan domainnya dalam komunikasi IoD. Melalui titik akses ini, lalu lintas jaringan dapat dimanipulasi oleh penyerang [92]. Ada berbagai solusi untuk mencegah serangan Man-in-the-Middle, yang termasuk enkripsi Strong Wired Equivalent Privacy (WEP)/WiFi Protected Access (WAP) pada titik akses, Hyper Text Transfer Protocol Secure (HTTPS), dan berbasis Kunci Publik otentikasi. • Pemalsuan pesan: Di bawah serangan pemalsuan pesan di IoD, pesan permintaan login sesi sebelumnya melalui saluran publik/terbuka dipalsukan selama eksekusi protokol otentikasi. Setelah itu, penyerang dapat memodifikasi dan mengirim ulang pesan ke pengguna.

3) Confidentiality: Kerahasiaan memastikan bahwa informasi tidak dapat bocor ke pengguna yang tidak sah. Banyak serangan terhadap IoD dan stasiun kontrol darat adalah akibat dari kekurangan dalam keamanan. Kerahasiaan dipengaruhi oleh akses pengguna yang tidak sah ke IoD dan itu mengambil informasi yang berguna.

a) Identity spoofing: Dalam spoofing identitas, penyerang berhasil menyamar sebagai pengguna yang sah di jaringan IoD dengan ID spoofing dari pengguna yang sah dan mendapatkan akses ke jaringan IoD dan tautan komunikasi. ID terenkripsi atau ID semu yang dapat digunakan satu kali dapat menjadi solusi yang efisien terhadap pencegahan serangan tersebut.

b) Akses tidak sah: Akses tidak sah adalah ketika seseorang memperoleh akses ke server IoD dan layanan menggunakan akun orang lain atau metode lain seperti ID duplikat. Serangan ini mengarah pada risiko pengungkapan informasi penting yang tidak sah dari IoD.

4) Availability: Ketersediaan didefinisikan sebagai layanan yang dimulai segera saat dibutuhkan untuk mempertahankan fungsi yang benar. Ketersediaan informasi adalah untuk memastikan bahwa pengguna yang sah dapat untuk mengakses

informasi berdasarkan kebutuhan mereka. IoD dioperasikan dalam orientasi misi bidang atau area, oleh karena itu, ketersediaan IoD menjadi perhatian utama dalam hal keamanan. Ketersediaan dapat dipengaruhi oleh faktor-faktor berikut.

a) Serangan fisik: Jenis serangan ini dilakukan pada komponen perangkat keras. Ini serangan memiliki motivasi utama untuk menghancurkan perangkat. Perangkat IoD mahal; oleh karena itu perlindungan terhadap serangan fisik adalah masalah yang cukup besar.

b) DoS dan DDoS: DoS didefinisikan sebagai menolak aksesibilitas sumber daya atau mencegah pengguna yang sah mengakses layanan dari sumber daya yang ditunjuk. IoD membutuhkan saluran komunikasi untuk mengirim dan menerima data [93]. Jika penyerang melakukan permintaan banjir pada saluran ini, jaringan terputus, yang menyebabkan tidak tersedianya sumber daya.

c) GPS spoofing: GPS digunakan untuk menentukan posisi kendaraan dan memberikan titik arah ke terbang ke sasaran yang ditentukan. Penyerang dapat mengubah konten sinyal GPS yang diterima atau menghasilkan sinyal spoofing dengan bantuan generator sinyal GPS

VII. Kesimpulan

Dari semua bagian yang sudah diberikan pembahasannya pada makalah ini, dapat diberi kesimpulan sebagai berikut. Parity Bit adalah salah satu cara untuk melakukan uji integritas file yang paling sederhana, tetapi pada penggunaannya terdapat kelemahan-kelemahan seperti jumlah bit yang sama-sama genap maupun ganjil tetapi berbeda dari yang aslinya akan dianggap tidak benar. Parity bit sendiri memiliki kelebihan seperti tidak memerlukan beban komputasi yang besar. Checksum sendiri merupakan istilah yang lebih luas dari algoritma-algoritma yang digunakan untuk melakukan pengecekan integritas. Terdapat banyak algoritma untuk melakukan checksum, salah satunya yang populer adalah MD5. MD5 merupakan algoritma hash function yang umum digunakan, meski sekarang hanya digunakan untuk sekedar melakukan cek integritas pada file yang tidak dimodifikasi secara sengaja. Hal ini terjadi karena komputer sekarang makin cepat sehingga metode brute force untuk menemukan collision dapat dengan mudah dilakukan. MD5 adalah varian dari message digest algorithm. SHA-1 merupakan generasi kedua dari keluarga SHA (Secure Hash Algorithm). SHA-1 juga sudah ditinggalkan karena alasan keamanan yang sama dengan MD5. SHA-2 merupakan hash function algorithm yang paling umum digunakan sekarang. NIST masih merekomendasikan SHA-2, namun disarankan menggunakan hash value yang besar agar semakin aman. SHA-2 juga dapat digunakan untuk melakukan pengecekan integritas file, namun apabila tidak memedulikan aspek sekuriti tidak disarankan karena beban komputasi yang lebih tinggi. SHA-3 merupakan terobosan terbaru dari keluarga SHA, karena menggunakan pendekatan yang berbeda dari varian sebelumnya, Keccak Algorithm. SHA-3 diyakini lebih aman dalam masalah anti collision, namun belum secara luas digunakan. CRC atau Cyclic Redundancy Check merupakan salah satu jenis checksum namun tidak diperuntukkan untuk keamanan. CRC bagus digunakan untuk melakukan verifikasi saat menyalin file ataupun pengarsipan file. Algoritma yang digunakan CRC juga terbilang tidak serumit MD5 dan SHA, sehingga pada *Integrated Ciruit* biasanya sudah diaplikasikan dan siap digunakan.

Pustaka

[1] J. Hu and A. Lanzon, "An innovative tri-rotor drone and associated distributed aerial drone swarm control," *Robotics and Autonomous Systems*, vol. 103, pp. 162–174, 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0921889017308163

[2] J. Cary, Leslie; Coyne, "Uas yearbook - uas: The global perspective," *ICAO Unmanned Aircraft Systems (UAS), Circular 328*, 2011-2012.

[3] "Unmanned aerial vehicles – the force multiplier of the 1990s," 2009. [Online]. Available: https://web.archive.org/web/20090724015052/http://www.airpower.maxwell.af.mil/airchronicles/apj/apj91/spr91/4spr91.htm

[4] J. Hu, P. Bhowmick, I. Jang, F. Arvin, and A. Lanzon, "A decentralized cluster formation containment framework for multirobot systems," *IEEE Transactions on Robotics*, vol. 37, no. 6, pp. 1936–1955, 2021.

[5] C. Koparan, A. B. Koc, C. V. Privette, and C. B. Sawyer, "Adaptive water sampling device for aerial robots," *Drones*, vol. 4, no. 1, 2020. [Online]. Available: https://www.mdpi.com/2504-446X/4/1/5

[6] C. Koparan, A. B. Koc, C. V. Privette, C. B. Sawyer, and J. L. Sharp, "Evaluation of a uav-assisted autonomous water sampling," *Water*, vol. 10, no. 5, 2018. [Online]. Available: https://www.mdpi.com/2073-4441/10/5/655

[7] C. Koparan, A. B. Koc, C. V. Privette, and C. B. Sawyer, "In situ water quality measurements using an unmanned aerial vehicle (uav) system," *Water*, vol. 10, no. 3, 2018. [Online]. Available: https://www.mdpi.com/2073-4441/10/3/264

[8] c. koparan, a. b. koc, c. v. privette, and c. b. sawyer, "autonomous in situ measurements of noncontaminant water quality indicators and sample collection with a uav," *water*, vol. 11, no. 3, 2019. [Online]. Available: https://www.mdpi.com/2073-4441/11/3/604

[9] "Drones smuggling porn, drugs to inmates around the world," 2017. [Online]. Available: http://www.foxnews.com/us/2017/04/17/drones-smuggling-porn-drugs-to-inmates-around-world.html

[10] M. Ayamga, S. Akaba, and A. A. Nyaaba, "Multifaceted applicability of drones: A review," *Technological Forecasting and Social Change*, vol. 167, p. 120677, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0040162521001098

[11] J. P. Rife, *The sound of freedom: Naval Weapons Technology at Dahlgren, Virginia 1918-2006*. Government Printing Office, 2006, vol. 6.

[12] L. Ramadass, S. Arunachalam, and Z. Sagayasree, "Applying deep learning algorithm to maintain social distance in public place through drone technology," *Int. J. Pervasive Comput. Commun.*, vol. 16, pp. 223–234, 2020.

[13] B. McCall, "Sub-saharan africa leads the way in medical drones," *The Lancet*, vol. 393, pp. 17–18, 01 2019.

[14] R. Kellermann, T. Biehle, and L. Fischer, "Drones for parcel and passenger transportation: A literature review," *Transportation Research Interdisciplinary Perspectives*, vol. 4, p. 100088, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2590198219300879

[15] B. Bolo, D. Mpoeleng, and I. Zlotnikova, "Development of methods acquiring real time very high resolution agricultural spatial information using unmanned aerial vehicle," *Agris on-line Papers in Economics and Informatics*, vol. 11, pp. 21–29, 06 2019.

[16] R. A. Clothier, D. A. Greer, D. G. Greer, and A. M. Mehta, "Risk perception and the public acceptance of drones," *Risk Analysis*, vol. 35, no. 6, pp. 1167–1183, 2015. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1111/risa.12330

[17] G. Sylvester, *E-agriculture in action: Drones for agriculture*. Food and Agriculture Organization ofn the United Nations and International ..., 2018.

[18] M. Gharibi, R. Boutaba, and S. L. Waslander, "Internet of drones," *IEEE Access*, vol. 4, pp. 1148–1162, 2016.

[19] G. Choudhary, V. Sharma, T. Gupta, J. Kim, and I. You, "Internet of drones (iod): threats, vulnerability, and security perspectives," *arXiv preprint arXiv:1808.00203*, 2018.

[20] S. Times, "Food delivery via drones in cyberjaya by end of the month," *Accessed: Apr*, vol. 4, p. 2020, 2020.

[21] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, H. Karimipour, G. Srivastava, and M. Aledhari, "Enabling drones in the internet of things with decentralized blockchain-based security," *IEEE Internet of Things Journal*, vol. 8, no. 8, pp. 6406–6415, 2020.

[22] A. D. Boursianis, M. S. Papadopoulou, P. Diamantoulakis, A. Liopa-Tsakalidi, P. Barouchas, G. Salahas, G. Karagiannidis, S. Wan, and S. K. Goudos, "Internet of things (iot) and agricultural unmanned aerial vehicles (uavs) in smart farming: a comprehensive review," *Internet of Things*, p. 100187, 2020.

[23] S. Magistretti and C. Dell'Era, "Unveiling opportunities afforded by emerging technologies: Evidences from the drone industry," *Technology Analysis & Strategic Management*, vol. 31, no. 5, pp. 606–623, 2019.

[24] D. Paddeu, T. Calvert, B. Clark, and G. Parkhurst, "New technology and automation in freight transport and handling systems," 2019.

[25] E. Vattapparamban, I. Güvenç, A. I. Yurekli, K. Akkaya, and S. Uluağaç, "Drones for smart cities: Issues in cybersecurity, privacy, and public safety," in *2016 international wireless communications and mobile computing conference (IWCMC)*. IEEE, 2016, pp. 216–221.

[26] M. Półka, S. Ptak, and Ł. Kuziora, "The use of uav's for search and rescue operations," *Procedia engineering*, vol. 192, pp. 748–752, 2017.

[27] V. Kharchenko and V. Torianyk, "Cybersecurity of the internet of drones: Vulnerabilities analysis and imeca based assessment," in *2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT)*. IEEE, 2018, pp. 364–369.

[28] F. Thiobane, "Cybersecurity and drones," Ph.D. dissertation, Utica College, 2015.

[29] M. Rodrigues, J. Amaro, F. S. Osório, and B. K. RLJC, "Authentication methods for uav communication," in *2019 IEEE Symposium on Computers and Communications (ISCC)*. IEEE, 2019, pp. 1210–1215.

[30] M. F. B. A. Rahman, "Smart cctvs for secure cities: Potentials and challenges," 2017.

[31] M. Mohan, "Cybersecurity in drones," Ph.D. dissertation, Utica College, 2016.

[32] M. Yahuza, M. Y. I. B. Idris, A. W. B. A. Wahab, A. T. Ho, S. Khan, S. N. B. Musa, and A. Z. B. Taha, "Systematic review on security and privacy requirements in edge computing: State of the art and future research opportunities," *IEEE Access*, vol. 8, pp. 76 541–76 567, 2020.

[33] S. Achanna, G. Krishnaswamy, P. Ponnampalam, and A. Bondhu, "Maternal mortality in malaysia: progress made towards millennium development goals (mdg) 5—an analysis of published data," *Med Res Archives*, vol. 6, 2018.

[34] R. Altawy and A. M. Youssef, "Security, privacy, and safety aspects of civilian drones: A survey," *ACM Transactions on Cyber-Physical Systems*, vol. 1, no. 2, pp. 1–25, 2016.

[35] D. He, S. Chan, and M. Guizani, "Drone-assisted public safety networks: The security aspect," *IEEE Communications Magazine*, vol. 55, no. 8, pp. 218–223, 2017.

[36] M. Yampolskiy, P. Horvath, X. D. Koutsoukos, Y. Xue, and J. Sztipanovits, "Taxonomy for description of cross-domain attacks on cps," in *Proceedings of the 2nd ACM international conference on High confidence networked systems*, 2013, pp. 135–142.

[37] H. Sedjelmaci and S. M. Senouci, "Cyber security methods for aerial vehicle networks: taxonomy, challenges and solution," *The Journal of Supercomputing*, vol. 74, no. 10, pp. 4928–4944, 2018.

[38] T. Humphreys, "Statement on the vulnerability of civil unmanned aerial vehicles and other systems to civil gps spoofing," *University of Texas at Austin (July 18, 2012)*, pp. 1–16, 2012.

[39] D. P. Shepard, J. A. Bhatti, T. E. Humphreys, and A. A. Fansler, "Evaluation of smart grid and civilian uav vulnerability to gps spoofing attacks," in *Proceedings of the 25th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2012)*, 2012, pp. 3591–3605.

[40] I. Güvenç, O. Ozdemir, Y. Yapici, H. Mehrpouyan, and D. Matolak, "Detection, localization, and tracking of unauthorized uas and jammers," in *2017 IEEE/AIAA 36th Digital Avionics Systems Conference (DASC)*. IEEE, 2017, pp. 1–10.

[41] R. L. Sturdivant and E. K. Chong, "Systems engineering baseline concept of a multispectral drone detection solution for airports," *IEEE Access*, vol. 5, pp. 7123–7138, 2017.

[42] X. Shi, C. Yang, W. Xie, C. Liang, Z. Shi, and J. Chen, "Anti-drone system with multiple surveillance technologies: Architecture, implementation, and challenges," *IEEE Communications Magazine*, vol. 56, no. 4, pp. 68–74, 2018.

[43] B. Nassi, A. Shabtai, R. Masuoka, and Y. Elovici, "Sok - security and privacy in the age of drones: Threats, challenges, solution mechanisms, and scientific gaps," 03 2019.

[44] J. Yao and N. Ansari, "Qos-aware power control in internet of drones for data collection service," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 7, pp. 6649–6656, 2019.

[45] C. Lin, D. He, N. Kumar, K.-K. R. Choo, A. Vinel, and X. Huang, "Security and privacy for the internet of drones: Challenges and solutions," *IEEE Communications Magazine*, vol. 56, no. 1, pp. 64–69, 2018.

[46] S. Aggarwal, M. Shojafar, N. Kumar, and M. Conti, "A new secure data dissemination model in internet of drones," in *ICC 2019-2019 IEEE International Conference on Communications (ICC)*. IEEE, 2019, pp. 1–6.

[47] B. Qureshi, A. Koubâa, M.-F. Sriti, Y. Javed, and M. Alajlan, "Dronemap-a cloud-based architecture for the internet-of-drones," in *International Conference on Embedded Wireless Systems and Networks*, 2016.

[48] P. Zhang, C. Wang, Z. Qin, and H. Cao, "A multidomain virtual network embedding algorithm based on multiobjective optimization for internet of drones architecture in industry 4.0," *Software: Practice and Experience*, 2020.

[49] K. M. Fornace, C. J. Drakeley, T. William, F. Espino, and J. Cox, "Mapping infectious disease landscapes: unmanned aerial vehicles and epidemiology," *Trends in parasitology*, vol. 30, no. 11, pp. 514–519, 2014.

[50] J. A. Barasona, M. Mulero-Pázmány, P. Acevedo, J. J. Negro, M. J. Torres, C. Gortázar, and J. Vicente, "Unmanned aircraft systems for studying spatial abundance of ungulates: relevance to spatial epidemiology," *PloS one*, vol. 9, no. 12, p. e115608, 2014.

[51] A. Priye, S. Wong, Y. Bi, M. Carpio, J. Chang, M. Coen, D. Cope, J. Harris, J. Johnson, A. Keller *et al.*, "Lab-on-a-drone: toward pinpoint deployment of smartphone-enabled nucleic acid-based diagnostics for mobile health care," *Analytical chemistry*, vol. 88, no. 9, pp. 4651–4660, 2016.

[52] K. S. Berns and S. P. Zietlow, "Blood usage in rotor-wing transport," *Air medical journal*, vol. 17, no. 3, pp. 105–108, 1998.

[53] G. L. Higgins, M. R. Baumann, K. M. Kendall, M. A. Watts, and T. D. Strout, "Red blood cell transfusion: experience in a rural aeromedical transport service," *Prehospital and disaster medicine*, vol. 27, no. 3, pp. 231–234, 2012.

[54] D. Jenkins, J. Stubbs, S. Williams, K. Berns, M. Zielinski, G. Strandenes, and S. Zietlow, "Implementation and execution of civilian remote damage control resuscitation programs," *Shock*, vol. 41, pp. 84–89, 2014.

[55] D. J. Riskin, T. C. Tsai, L. Riskin, T. Hernandez-Boussard, M. Purtill, P. M. Maggio, D. A. Spain, and S. I. Brundage, "Massive transfusion protocols: the role of aggressive resuscitation versus product ratio in mortality reduction," *Journal of the American College of Surgeons*, vol. 209, no. 2, pp. 198–205, 2009.

[56] B. Mitra, A. Mori, P. A. Cameron, M. Fitzgerald, E. Paul, and A. Street, "Fresh frozen plasma (ffp) use during massive blood transfusion in trauma resuscitation," *Injury*, vol. 41, no. 1, pp. 35–39, 2010.

[57] H. F. Pidcoke, J. K. Aden, A. G. Mora, M. A. Borgman, P. C. Spinella, M. A. Dubick, L. H. Blackbourne, and A. P. Cap, "Ten-year analysis of transfusion in operation iraqi freedom and operation enduring freedom: increased plasma and platelet use correlates with improved survival," *Journal of Trauma and Acute Care Surgery*, vol. 73, no. 6, pp. S445–S452, 2012.

[58] K. Reid-Lombardo, C. C. Glass, S. G. Marcus, J. Liesinger, D. B. Jones *et al.*, "Workforce shortage for general surgeons: results from the society for surgery of the alimentary track (ssat) surgeon shortage survey," *Journal of Gastrointestinal Surgery*, vol. 18, no. 12, pp. 2061–2073, 2014.

[59] E. J. MacKenzie, D. B. Hoyt, J. C. Sacra, G. J. Jurkovich, A. R. Carlini, S. D. Teitelbaum, and H. Teter Jr, "National inventory of hospital trauma centers," *Jama*, vol. 289, no. 12, pp. 1515–1522, 2003.

[60] C. C. Branas, E. J. MacKenzie, J. C. Williams, C. W. Schwab, H. M. Teter, M. C. Flanigan, A. J. Blatt, and C. S. ReVelle, "Access to trauma centers in the united states," *Jama*, vol. 293, no. 21, pp. 2626–2633, 2005.

[61] "American red cross. blood components," 2014. [Online]. Available: https://www.researchgate.net/deref/http%3A%2F%2Fwww.redcrossblood.org%2Flearn-about-blood%2Fblood-components

[62] N. J. Krumrei, M. S. Park, B. A. Cotton, and M. D. Zielinski, "Comparison of massive blood transfusion predictive models in the rural setting,"

Journal of Trauma and Acute Care Surgery, vol. 72, no. 1, pp. 211–215, 2012.

[63] J. B. Holcomb, L. A. Zarzabal, J. E. Michalek, R. A. Kozar, P. C. Spinella, J. G. Perkins, N. Matijevic, J.-F. Dong, S. Pati, C. E. Wade *et al.*, "Increased platelet: Rbc ratios are associated with improved survival after massive transfusion," *Journal of Trauma and Acute Care Surgery*, vol. 71, no. 2, pp. S318–S328, 2011.

[64] P. J. Schmidt, "Blood and disaster–supply and demand." *The New England journal of medicine*, vol. 346, no. 8, pp. 617–620, 2002.

[65] M. L. Erickson, M. H. Champion, R. Klein, R. L. Ross, Z. M. Neal, and E. L. Snyder, "Management of blood shortages in a tertiary care academic medical center: the yale-new haven hospital frozen blood reserve," *Transfusion*, vol. 48, no. 10, pp. 2252–2263, 2008.

[66] H. Abolghasemi, M. H. Radfar, M. Tabatabaee, N. S. Hosseini-Divkolayee, and F. M. Burkle, "Revisiting blood transfusion preparedness: experience from the bam earthquake response," *Prehospital and disaster medicine*, vol. 23, no. 5, pp. 391–394, 2008.

[67] H. G. Klein, "Earthquake in america." *Transfusion*, vol. 41, no. 10, pp. 1179–1180, 2001.

[68] M. Galloway, G. Jane, L. Sudlow, J. Trattles, and J. Watson, "A tabletop exercise to assess a hospital emergency blood management contingency plan in a simulated acute blood shortage," *Transfusion medicine*, vol. 18, no. 5, pp. 302–307, 2008.

[69] S. G. Sandler and G. J. Ouellette, "Transportation and other blood system issues related to disasters: Washington, dc experience of september 11, 2002," *Vox sanguinis*, vol. 83, pp. 367–370, 2002.

[70] J. Hlad, "Drones: A force for good when flying in the face of disaster," *The Guardian. July*, vol. 8, 2015.

[71] J. C. Rosser Jr, V. Vignesh, B. A. Terwilliger, and B. C. Parker, "Surgical and medical applications of drones: A comprehensive review," *JSLS: Journal of the Society of Laparoendoscopic Surgeons*, vol. 22, no. 3, 2018.

[72] A. Capolupo, S. Pindozzi, C. Okello, N. Fiorentino, and L. Boccia, "Photogrammetry for environmental monitoring: The use of drones and hydrological models for detection of soil contaminated by copper," *Science of the Total Environment*, vol. 514, pp. 298–306, 2015.

[73] J. M. Brady, M. D. Stokes, J. Bonnardel, and T. H. Bertram, "Characterization of a quadrotor unmanned aircraft system for aerosol-particle-concentration measurements," *Environmental science & technology*, vol. 50, no. 3, pp. 1376–1383, 2016.

[74] X.-B. Tang, J. Meng, P. Wang, Y. Cao, X. Huang, L.-S. Wen, and D. Chen, "Efficiency calibration and minimum detectable activity concentration of a real-time uav airborne sensor system with two gamma spectrometers," *Applied Radiation and Isotopes*, vol. 110, pp. 100–108, 2016.

[75] P. G. Martin, O. D. Payton, J. S. Fardoulis, D. A. Richards, and T. B. Scott, "The use of unmanned aerial systems for the mapping of legacy uranium mines," *Journal of environmental radioactivity*, vol. 143, pp. 135–140, 2015.

[76] G.-M. Breen and J. Matusitz, "An evolutionary examination of telemedicine: A health and computer-mediated communication perspective," *Social work in public health*, vol. 25, no. 1, pp. 59–71, 2010.

[77] J. Rosser, M. Wood, J. Payne, T. Fullum, G. Lisehora, L. Rosser, P. Barcia, and R. Savalgi, "Telementoring," *Surgical endoscopy*, vol. 11, no. 8, pp. 852–855, 1997.

[78] B. M. Harnett, C. R. Doarn, J. Rosen, B. Hannaford, and T. J. Broderick, "Evaluation of unmanned airborne vehicles and mobile robotic telesurgery in an extreme environment," *Telemedicine and e-Health*, vol. 14, no. 6, pp. 539–544, 2008.

[79] J. Euchi, "Do drones have a realistic place in a pandemic fight for delivering medical supplies in healthcare systems problems?" pp. 182–190, 2021.

[80] E. Dahlman and K. Lagrelius, "A game of drones: Cyber security in uavs," 2019.

[81] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Transactions on information theory*, vol. 29, no. 2, pp. 198–208, 1983.

[82] R. Canetti and H. Krawczyk, "Universally composable notions of key exchange and secure channels," in *International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 2002, pp. 337–351.

[83] B. Potteiger, G. Martins, and X. Koutsoukos, "Software and attack centric integrated threat modeling for quantitative risk assessment," in *Proceedings of the Symposium and Bootcamp on the Science of Security*, 2016, pp. 99–108.

[84] B. Schneier, "Attack trees," *Dr. Dobb's journal*, vol. 24, no. 12, pp. 21–29, 1999.

[85] Y. Tian, J. Yuan, and H. Song, "Efficient privacy-preserving authentication framework for edge-assisted internet of drones," *Journal of Information Security and Applications*, vol. 48, p. 102354, 2019.

[86] C.-L. Chen, Y.-Y. Deng, W. Weng, C.-H. Chen, Y.-J. Chiu, and C.-M. Wu, "A traceable and privacy-preserving authentication for uav communication control system," *Electronics*, vol. 9, no. 1, p. 62, 2020.

[87] B. Bera, A. K. Das, and A. K. Sutrala, "Private blockchain-based access control mechanism for unauthorized uav detection and mitigation in internet of drones environment," *Computer Communications*, vol. 166, pp. 91–109, 2021.

[88] M. Wazid, A. K. Das, N. Kumar, A. V. Vasilakos, and J. J. Rodrigues, "Design and analysis of secure lightweight remote user authentication and key agreement scheme in internet of drones deployment," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 3572–3584, 2018.

[89] Y. Aydin, G. K. Kurt, E. Ozdemir, and H. Yanikomeroglu, "Group handover for drone-mounted base stations," *IEEE Internet of Things Journal*, 2021.

[90] A. A. M. A. Abdelhafez, "Localization of cyber-physical systems: privacy, security and efficiency," Ph.D. dissertation, Technische Universität München, 2020.

[91] K. Hartmann and C. Steup, "The vulnerability of uavs to cyber attacks-an approach to the risk assessment," in *2013 5th international conference on cyber conflict (CYCON 2013)*. IEEE, 2013, pp. 1–23.

[92] S. Kamthan, H. Singh, and T. Meitzler, "Uavs: on development of fuzzy model for categorization of countermeasures during threat assessment," in *Unmanned Systems Technology XIX*, vol. 10195. International Society for Optics and Photonics, 2017, p. 1019518.

[93] N. M. Rodday, R. d. O. Schmidt, and A. Pras, "Exploring security vulnerabilities of unmanned aerial vehicles," in *NOMS 2016-2016 IEEE/IFIP Network Operations and Management Symposium*. IEEE, 2016, pp. 993–994.