Optimasi Keamanan Autentikasi dari *Man in the Middle Attack* (MiTM) Menggunakan Teknologi Blockchain

Imam Riadi[1], Rusydi Umar[2], Iqbal Busthomi[3]

[1]Program Studi Sistem Informasi, Universitas Ahmad Dahlan, Indonesia
[2,3]Program Studi Teknik Informatika, Universitas Ahmad Dahlan, Indonesia
[1]imam.riadi@is.uad.ac.id
[2]rusydi@mti.uad.ac.id
[3]iqbal1907048011@webmail.uad.ac.id

***Abstrak*— Teknologi informasi memberikan dampak yang besar dalam aspek bisnis. Sistem informasi merupakan salah satu dampak dari kemajuan teknologi yang menjadi salah satu sarana untuk memudahkan pengelolaan informasi dan pelaporan pada sebuah perusahaan. Sistem informasi menggunakan proses autentikasi sebagai gerbang depan untuk melakukan validasi user sebelum mendapatkan layanan. Proses autentikasi memiliki kerentanan dari serangan siber, diantaranya adalah *Man-in-the-middle attack*. *Payload* autentikasi yang dikirim dan diterima pada sebuah sistem informasi perlu diamankan dengan baik. Pengiriman payload autentikasi dalam bentuk *plaintext* rentan akan serangan *Man-in-the-middle*. Teknologi Blockchain memberikan solusi keamanan berupa mekanisme blok hash untuk mengamankan data *payload*. *Payload* autentikasi sebelum dikirmkan diubah menjadi blok hash, sehingga keamanan dan kerahasiaan data payload lebih terjamin.**

***Kata Kunci*— Autentikasi, *Man-in-the-middle attack*, Teknologi Blockchain, Hash, *Payload*.**

I. PENDAHULUAN

Teknologi berkembang dengan sangat pesat, hingga menjadikan teknologi sebagai sarat dalam komunikasi dan berbagi informasi. Kemajuan teknologi memberikan peranan penting dalam memberikan sumber data [1]. Teknologi informasi mengolah data-data yang ada menjadi sebuah informasi.

Teknologi informasi membawa dunia bisnis menjadi lebih ringkas, karena kecanggihan teknologi tak hanya memangkas waktu tetapi juga menjadi perantara komunikasi. Sebagai contoh seperti kantor pos kini tidak lagi relevan karena komunikasi menggunakan jaringan informasi memberikan layanan yang lebih cepat, sehingga kini kantor pos lebih berfungsi sebagai jasa pengantar barang daripada perantara pengiriman surat [2].

Dampak Perkembangan teknologi mengiringi perkembangan perusahaan dan bisnis yang lebih deikenal dengan sebutan *e-commerce*. Kemudahan yang ditimbulkan dari munculnya *e-commerce* mengundang orang-orang yang memiliki jiwa wirausaha kemudian berlomba-lomba mendirikan perusahaan pemula atau biasa di sebut dengan perusahaan *startup*. *Startup* identik dengan pemula bisnis (belum lama beroperasi) dan masih dalam proses pengembangan dalam memilih pasar dari bisnis yang dibangun, tetapi pada kenyataanya *startup* lebih seperti menjadi perusahaan yang bergerak dengan memaksimalkan kinerja teknologi informasi dan internet karena biasanya berfokus pada penggunaan website dan sistem informasi [3].

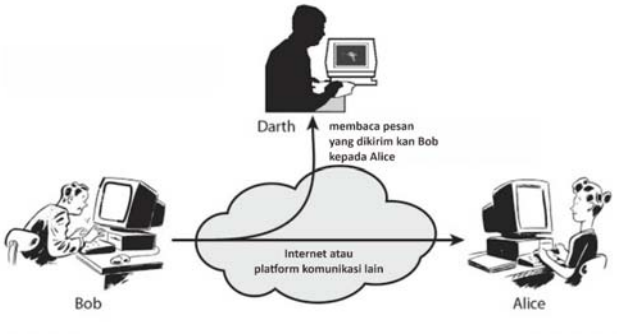
Sistem informasi merupakan sebuah aplikasi yang digunakan dalam sebuah organisasi yang sebagai pendukung pengelolaan transaksi hingga pelaporan [4]. Autentikasi merupakan gerbang utama dalam sebuah sistem informasi, sehingga dapat mendapatkan layanan sesuai dengan hak akses yang diberikan kepada user tersebut [5]. Proses autentikasi merupakan proses validasi user pada saat memasuki sistem dan memungkinkan user untuk mengakses seluruh layanan yang diberikan pleh sistem tanpa perlu memasukkan passwordnya berulang kali [6], [7].

Keamanan informasi merupakan aspek penting yang perlu diperhatikan dalam membangun sistem [6]. Proses autentikasi yang merupakan gerbang depan dalam sebuah sistem informasi memiliki celah dan kerentanan, diantaranya proses pengiriman dan penerimaan *payload* dari server dalam bentuk *plaintext* [7]. Keamanan pada proses autentikasi perlu ditingkatkan guna menanggulagi serangan-serangan siber seperti *Cross Site Scripting* (XSS), *Sniffing*, dan juga serangan *Man-in-the-middle* [8].

Man-in-the-middle attacks adalah salah satu serangan pada jaringan dengan akses terbuka [8]. *Man-in-the-middle attacks* merupakan serangan yang pada dasarnya penyerang memasukkan dirinya di antara dua pihak atau perangkat dalam mode sembunyi-sembunyi sehingga semua paket yang berlintas antara kedua pihak yang sah itu dialihkan melalui penyerang tersebut. Serangan ini cukup berbahaya karena penyerang kemudian dapat mengubah informasi dari paket yang dikirimkan, dan berpotensi mengirim data yang dipalsukan ke salah satu pihak [9].

Man-in-the-middle attacks didapatkan dari situasi bola di mana dua pemain bermaksud saling mengoper bola, sementara satu pemain di antara mereka mencoba merebutnya. *Man-in-the-middle attacks* berfokus pada informasi yang mengalir di antara titik akhir, kerahasiaan dan kebenaran informasi tersebut. *Man-in-the-middle attacks* adalah proses menyadap di mana dalam komunikasi antara dua perangkat A dan B, penyerang menerima A dengan berpura-pura dia adalah B. Ini berarti setiap kali A ingin mengirim pesan ke B, itu sebenarnya mengirimkannya ke penyerang yang membaca pesan kemudian meneruskannya ke B untuk membuat komunikasi tetap berfungsi. Penyerang dapat membaca semua

konten komunikasi termasuk email, gambar, dan password[9], [10]. Proses *Man-in-the-middle attacks* digambarkan pada Gbr. 1 [11].



Gbr. 1 Visualisasi *Man-in-the-middle attacks.*

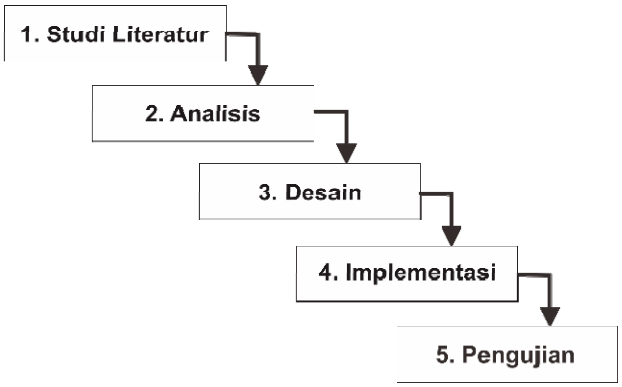
Teknologi Blockchain merupakan kumpulan beberapa konsep keamanan yang dapat digunakan untuk menjamin kerahasiaan informasi [12]. Salah satu konsep yang digunakan teknologi Blockchain seperti konsep yang digunakan pada *distributed database* [13]. Konsep *distributed database* dari teknologi Blockchain adalah dimana *database* yang terdistribusi berisi catatan transaksi yang dibagikan di antara anggota yang berpartisipasi pada *chain* tersebut. Setiap transaksi dikonfirmasi oleh konsensus mayoritas dari anggota, sehingga membuat transaksi penipuan tidak dapat terjadi. Blockchain merupakan sebuah kumpulan blok yang membentuk rantai (*chain*). Setiap blok memiliki 3 elemen yaitu data, nilai *hash* dari blok, dan nilai *previous hash* atau nilai *hash* dari blok sebelumnya. Teknik memanfaatkan *hash* inilah yang membuat Blockchain menjadi lebih aman, karena jika ada yang mengubah salah satu blok dalam rantai blok maka nilai *hash*-nya akan berubah dan blok berikutnya akan menjadi tidak valid lagi karena tidak menyimpan nilai *hash* yang valid dari blok sebelumnya. Artinya, perubahan yang dilakukan terhadap sebuah blok akan mengakibatkan seluruh rantai blok menjadi tidak valid [14], [15].

Teknologi Blockchain menyimpan data dalam bentuk *hash*, membuat data menjadi tersamarkan sehingga informasi yang terkandung dalam blok tersebut dapat tersembunyi [16]. Teknologi ini juga mampu mencegah adanya perubahan atau pemalsuan transaksi sehingga dapat digunakan untuk melakukan transaksi secara langsung secara aman. Sistem pencatatan logs yang terdistribusi dan transparan dari teknologi ini dapat menjadi solusi untuk diterapkan pada pencatatan transaksi sehingga dapat menjadi upaya untuk meminimalisir tingkat pemalsuan dan penyalahgunaan data [3].

Berdasarkan kerentanan yang diidentifikasi maka teknologi Blockchain memiliki potensi untuk dapat menanggulagi berbagai serangan. Percobaan serangan *Man-in-the-middle attacks* dapat dilakukan untuk menguji teknologi Blockchain dalam melindungi dan menjaga kerahasiaan data dari *attacker*.

II. METODOLOGI PENELITIAN

Metodologi yang digunakan pada penelitian ini merupakan metode *patching*, dimana objek yang akan diteliti sebelumnya sudah ada namun dilakukan *updating* untuk menyempurnakan objek tersebut. Adapun langkah-langkah metode *patching* dapat dilihat pada Gbr. 2.

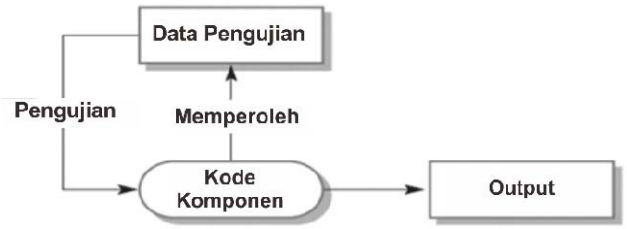


Gbr. 2 Visualisasi langkah-langkah metode *patching.*

Langkah-langkah *patching* dapat dibagi atas 5 tahapan. Tahap studi literatur, analisis, desain, implementasi dan *testing* atau pengujian yang diuraikan sebagai berikut:

1. Studi literatur, pada tahap ini dilakukan pengumpulan data baik mengenai sistem yang akan digunakan untuk penelitian, dasar teori baik mengenai *Man-in-the-middle attacks*, teori Blockchain, hingga *tools* yang akan digunakan dalam penelitian. Pengumpulan literatur terbagi atas 2 sumber, yakni dari jurnal penelitian yang berkaitan dan internet.
2. Analisis, tahap ini merupakan tahap untuk melakukan analisis kondisi saat ini mengenai sistem yang akan digunakan dalam penelitian ini, baik dari bagaimana sistem bekerja, alur sistem hingga *payload* data yang akan menjadi fokus utama pada penelitian ini. Selain itu juga percobaan *Man-in-the-middle attacks* menggunakan *tools* Burpsuite v.2020.1, sebelum diimplementasikan konsep pengamanan yang ditawarkan. Tujuan dari tahap ini adalah mendapat semua detail dari sistem yang digunakan saat ini [17].
3. Desain, hasil analisis tentu saja akan lebih jelas jika digambarkan dengan skema proses atau desain alur, sehingga pada tahap ini akan dipaparkan dan ditampilkan gambaran mengenai proses serangan dan pengamanan data yang dilakukan.
4. Implementasi, tahap ini merupakan percobaan pengimplementasian dari hasil analisis [17], kerentanan yang akan terjadi ketika sistem tersebut dianalisis akan diimplementasikan teknologi Blockchain untuk mengamankan informasi pada sistem terebut.
5. Testing, tahap ini merupakan tahap pengujian dari implementasi teknologi Blockchain yang telah dilakukan. Metode pengujian yang dilakukan adalah *White Box*

Testing seperti yang dipaparkan pada Gbr. 3 [18]. *White Box Testing* adalah metode *test case* yang sepenuhnya dikendalikan oleh pengembang [19]. *White Box Testing* sangat meningkatkan efektivitas *testing* secara keseluruhan, hal ini dapat lebih mudah mendeteksi *bug* yang sulit ditemukan dengan pengujian *Black Box Testing* atau metode pengujian lainnya, oleh karena itu Seorang *White Box Tester* harus memiliki pengetahuan mengenai struktur pemrograman [20], [21]. Pengujian yang akan dilakukan adalah percobaan serangan langsung menggunakan *Man-in-the-middle attack.*



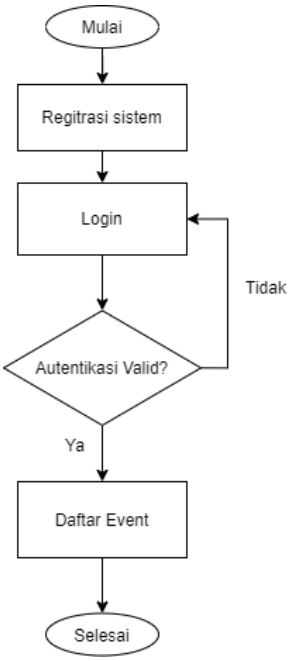
Gbr. 3 *White Box Testing.*

III. HASIL DAN PEMBAHASAN

Objek dari penelitian ini adalah proses autentikasi dari Sistem Nyebar yang digunakan oleh CV. Nyebar Inspirasi Nusantara. Sistem Nyebar merupakan aplikasi yang menjadi sebagai wadah utama untuk mengelola data-data *event*, mulai dari registrasi akun, pendaftaran event, registrasi ualng, pembayaran, hingga *feedback* dari penyelenggaraan event tersebut.

Sistem Nyebar menyediakan layanan pendaftaran akun default sebagai Member, dimana akun tersebut dapat di-*uprade* menjadi akun *Organizer* yang dapat merupakan sebuah lembaga baik profit maupun non-profit. Akun *Organizer* memiliki *privilege* untuk menyelenggarakan dan mempublikasikan event di Sistem Nyebar, mengelola data pendaftaran, dan mengelola data *feedback* dari Member, sehingga Member yang dapat mendaftarkan diri pada event-event yang tersedia.

Gbr. 4 memaparkan proses pendaftaran event seorang Member. Sebelum mendaftatr sebuah event yang ada pada Sistem Nyebar, Member harus melakukan validasi data berupa memasukkan *username* dan password atau metode lain yang digunakan untuk validasi akun. Member yang telah berhasil masuk kedalam akun dapat melakukan pendaftaran event yang di selenggarakan oleh *Organizer*



Gbr. 4 *Flowchart* Proses Pendaftaran Event.

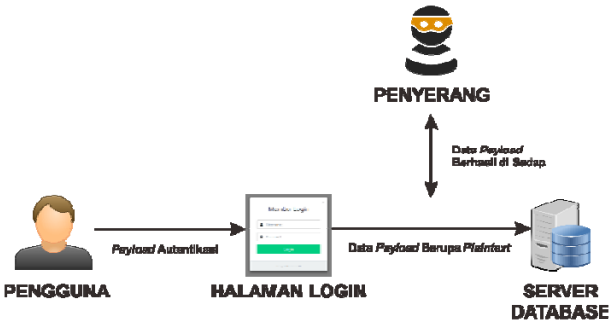
Saat ini Sistem Nyebar belum diamankan dengan baik seperti yang terlihat pada Gbr. 5. Pada Gambar tersebut terlihat bahwa *payload* data autentikasi yang dikirim masih dalam bentuk *plaintext*, sehingga data-data tersebut langsung dapat dilihat *value*-nya oleh penyerang. Data yang belum diberlakukan pengamanan yang baik dapat menyebabkan data tersebut mudah untuk disadap dan nantinya akan berdampak pada penyalahgunaan data tersebut.

Berdasarkan analisis yang dilakukan, memperoleh hasil mengenai gambaran konseptual dari proses autentikasi pada Sistem Nyebar yang dapat dilihat pada Gbr. 6. User harus melakukan autentikasi terlebih dahulu untuk mengakses Sistem Nyebar. Autentikasi yang diperlukan berupa memasukka *username* dan password dari akun yang telah terdaftar. Kondisi saat ini seperti yang telah dipaparkan pada Gbr. 5 bahwa Sistem Nyebar ketika melakukan POST data untuk autentikasi masih berupa *plaintext*, sehingga ketika dilakukan *sniffing* pada proses tersebut akan didapatkan *username* dan password yang diinputkan.

POST request to //t.co/fCUxNHP2Xh

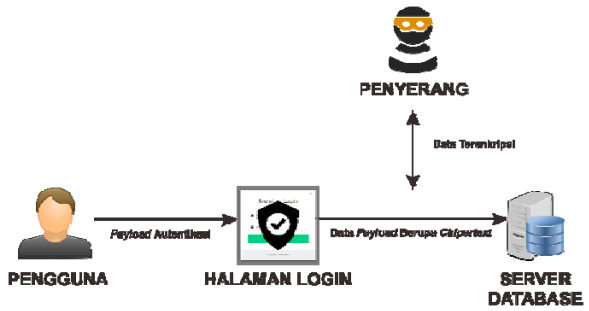
Type	Name	Value
URL	amp	1/signup
Body	email	admin
Body	password	admin

Gbr. 5 *Capture Payload* Proses Autentikasi Admin.



Gbr. 6 Konseptual Hasil Analisis Kondisi Sistem Nyebar.

Gbr. 7 memaparkan menegenai konseptual rancangan solusi keamanan dari permasalahan yang ada. Gambaran rancangan keamanan yang akan dilakukan adalah menambah *patch* pada *form* autentikasi sehingga data yang akan dikirimkan dapat diamankan, sehingga penyerang tidak dapat membaca isi *payload* data yang dikirimkan oleh pengguna.



Gbr. 7 Konseptual Rancangan Keamanan yang akan Diimplementasikan.

Teknologi Blockchain memiliki beberapa mekanisme pengamanan diantaranya pengamanan menggunakan algoritma kriptografi dengan mekanisme blok hash, *proof-of-work*, dan mekanisme penyimpanan terdistribusi [14]. Kondisi saat ini dari Sistem Nyebar adalah tidak adanya pengamanan *payload* autentikasi sehingga masih dikirimkan dalam bentuk *plaintext*, oleh karena itu mekanisme blok hash dari teknologi Blockchain memberikan peluang untuk membuat pengiriman *payload* autentikasi menjadi lebih aman.

Algoritma pembuatan blok hash dapat dilihat pada Gbr. 8. Blok hash akan dibuat ketika proses registrasi akun dan akan tersimpan dalam bentuk blok hash yang dapat digunakan untuk autentikasi user. Adapun blok hash yang akan di-*generate* berisi 0 yang merupakan *key* dari blok, *username*, dan password. *Username* adalah elemen unik sehingga dapat menanggulangi duplikasi data pada server.

```
authHash() {
   return SHA256(
      0 + this.email + this.password
   ).toString();
}
```

Gbr. 8 Algoritma Pembuatan Blok Hash.

Percobaan POST data registrasi setelah diamankan menggunakan teknogi Blockchain membuat data yang dikirimkan menjadi sebuah blok hash, sehingga data asli menjadi lebih aman dan rahasia. Data yang di POST akan disimpan ke dalam *database* server, seperti yang terlihat pada Gbr. 9.

Hasil pengujian dari *White Box Testing* dapat dilihat pada Gbr. 10. Pengujian dengan percobaan serangan *Man-in-the-middle* pada proses autentikasi menggunakan *tools* Burpsuite v.2020.1 menghasilkan *payload* data yang dikirimkan berupa blok hash atau terenkripsi, sehingga data yang terkandung dalam payload tersebut lebih terjamin keamananya dan terjaga kerahasiaanya. Gbr. 11 memaparkan status autentikasi setelah teknologi Blockchain diimplementasikan pada Sistem Nyebar.


```
{
    "status": 200,
    "result": {
        "_id": "5e70a8059b9b796073885924",
        "auth_hash": "9004e53d1304e17aa46072aa77169523660fa5c60cb2bc82f2d5aea9bc629fb7",
        "createdAt": "2020-03-17T10:35:49.121Z",
        "updatedAt": "2020-03-17T10:35:49.121Z",
        "__v": 0
    }
}
```


Gbr. 9 Data Autentikasi User yang Tersimpan di *Database*.

Gbr. 10 *Payload* Data Autentikasi User yang di *Capture* Menggunakan Burpsuite.

```
{
    "status": 200,
    "message": "Login success",
    "result": {
        "_id": "5e70a8059b9b796073885924",
        "auth_hash": "9004e53d1304e17aa46072aa77169523660fa5c60cb2bc82f2d5aea9bc629fb7",
        "createdAt": "2020-03-17T10:35:49.121Z",
        "updatedAt": "2020-03-17T10:35:49.121Z",
        "__v": 0
    }
}
```


Gbr. 11 Status Autentikasi Setelah Diimplementasikan Teknologi Blockchain.

IV. KESIMPULAN

Keamanan sistem informasi merupakan aspek yang sangat perlu untuk diperhatikan untuk menjaga data yang dikelola pada sistem tersebut. Autentikasi sebagai gerbang utama dalam sebuah sistem informasi, sehingga kerentanan-kerentanan dalam sebuah proses autentikasi harus ditanggulangi. Serangan Man-in-the-middle sebagai salah satu serangan yang dapat membuka celah kerentanan proses autentikasi. Teknologi Blockchain memiliki mekanisme blok hash yang dapat digunakan untuk menutup celah kerentanan pada proses autentikasi. Mekanisme blok hash mengubah data payload autentikasi yang berupa plaintext menjadi data chipertext dengan mengubah data tersebut menjadi blok enkripsi. Blok data tersebut tidak dapat dibaca sehingga dapat menjamin keamanan dan kerahasiaan data payload. Berdasarkan hasil yang didapatkan maka implementasi dari teknologi Blockchain berhasil mengamankan data payload autentikasi pada sebuah sistem informasi.

REFERENSI

[1] I. Riadi, R. Umar, and I. M. Nasrulloh, "Analisis Forensik Digital Pada Frozen Solid State Drive Dengan Metode National Institute of Justice (NIJ)," *Elinvo (Electronics, Informatics, and Vocational Education)*, vol. 3, no. 1, pp. 70–82, 2018, doi: 10.21831/elinvo.v3i1.19308.

[2] A. Fauzan N I, "Teknologi Blockchain dan Peranannya dalam Era Digital," *Jurnal BJB University*, vol. 4, pp. 1–15, 2018.

[3] M. D. K. Perdani, W. Widyawan, and P. I. Santosa, "Blockchain untuk Keamanan Transaksi Elektronik Perusahaan Financial Technology (Studi Kasus pada PT XYZ)," *Semnasteknomedia*, vol. 6, no. 1, pp. 7–12, 2018.

[4] F. Septa and R. Umar, "Analisis kepuasan pengguna sistem informasi e-government menggunakan metode webqual 4.0 (studi kasus: website simsarpras kementerian agama)," *METHOMIKA: Jurnal Manajemen Informatika & Komputerisasi Akuntansi*, vol. 3, no. 2, 2019.

[5] C. E. Suling, M. Olivya, and R. Nur, "Prototype Pengembangan Autentikasi Login Menggunakan Teknologi Quick Respone Code," in *Seminar Nasional Teknik Elektro dan Informatika (SNTEI) 2017*, 2017, no. November, pp. 156–161.

[6] R. Firdaus, D. Kurniawan, and E. C. Simamora, "Implementasi metode autentikasi one time password (otpa) berbasis mobile token pada aplikasi ujian online (studi kasus : jurusan matematika fmipa unila)," in *Prosiding SNSMAIP III-2012*, 2012.

[7] R. Munadi, Z. Musliyana, and T. Y. Arif, "Peningkatan Sistem Keamanan Otentikasi Single Sign On (SSO) Menggunakan Algoritma AES dan One-Time Password Studi Kasus: SSO Universitas Ubudiyah Indonesia," *Jurnal Rekayasa Elektrika*, vol. 12, no. 1, pp. 21–29, 2016.

[8] D. Saputra and I. Riadi, "Network Forensics Analysis of Man in the Middle Attack Using Live Forensics Method," *International Journal of Cyber-Security and Digital Forensics*, vol. 8, no. 1, pp. 66–73, 2019, doi: 10.17781/p002558.

[9] R. A. Sowah, K. B. Ofori-Amanfo, G. A. Mills, and K. M. Koumadi, "Detection and prevention of man-in-the-middle spoofing attacks in MANETs using predictive techniques in Artificial Neural Networks (ANN)," *Journal of Computer Networks and Communications*, vol. 2019, 2019, doi: 10.1155/2019/4683982.

[10] P. Radhika, G. Ramya, K. Sadhana, and R. Salini, "Defending Man In The Middle Attacks," *International Research Journal of Engineering and Technology(IRJET)*, vol. 4, no. 3, pp. 579–585, 2017.

[11] William Stallings, *Cryptography and Network Security*, 4th ed. Prentice Hall, 2005.

[12] G. D. Putra, S. Sumaryono, and W. Widyawan, "Rancang Bangun Identity and Access Management IoT Berbasis KSI dan Permissioned Blockchain," *Jurnal Nasional Teknik Elektro dan Teknologi Informasi (JNTETI)*, vol. 7, no. 4, pp. 384–390, 2018, doi: 10.22146/jnteti.v7i4.455.

[13] Caroline Harris, "The History of Bitcoin," 2019. [Online]. Available: https://cryptocurrencynews.com/the-history-of-bitcoin/. [Accessed: 24-Feb-2020].

[14] R. C. Noorsanti, H. Yulianton, and K. Hadiono, "Blockchain - Teknologi Mata Uang Kripto (Crypto Currency)," *Prosiding SENDI_U*, vol. 3, p. 306, 2018.

[15] D. Efanov and P. Roschin, "The All-Pervasiveness of the Blockchain Technology," in *Procedia Computer Science*, 2018, pp. 116–121, doi: https://doi.org/10.1016/j.procs.2018.01.019.

[16] R. Zhang, R. Xue, and L. Liu, "Security and privacy on blockchain," *ACM Computing Surveys*, vol. 52, no. 3, 2019, doi: 10.1145/3316481.

[17] S. Barjtya, A. Sharma, and U. Rani, "A detailed study of Software Development Life Cycle (SDLC) Models," *International Journal Of Engineering And Computer Science ISSN*, vol. 6, no. 7, pp. 22097–22100, 2017, doi: 10.18535/ijecs/v6i7.32.

[18] Ian Sommerville, *Software Engineering, 9th Edition*, 9th ed. Scotland: University of St Andrews, 2011.

[19] Y. Irawan, "Pengujian Sistem Informasi Pengelolaan Pelatihan Kerja UPT BLK Kabupaten Kudus dengan Metode Whitebox Testing," *Sentra Penelitian Engineering dan Edukasi*, vol. 9, no. 3, pp. 59–63, 2017.

[20] S. Alfisahrin, "Pendekatan White Box Testing Untuk Menentukan Kualitas Perangkat Lunak Dengan Menggunakan Bahasa Pemrograman C++," *Paradigma*, vol. XIV, no. 1, pp. 69–78, 2012.

[21] H. B. I. Alfaris, C. Anam, and A. Masy'an, "Implementasi Black Box Testing Pada Sistem Informasi Pendaftaran Santri Berbasis Web Dengan Menggunakan PHP Dan MYSQL," *Jurnal Sains dan Teknologi*, vol. 6, no. 1, pp. 23–38, 2013.