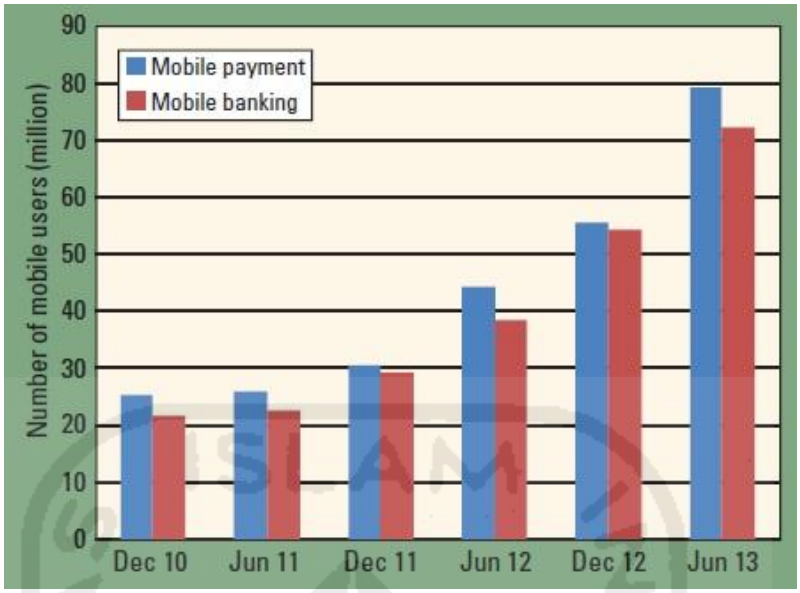
Bab 2 Tinjauan Pustaka

2.1. Penelitian Terdahulu

Penelitian yang terkait dengan *mobile forensics* telah banyak dilakukan, terlebih saat ini banyak sekali fungsi serta kegunaan dari perangkat *smartphone* atau perangkat *mobile* lainnya. Jika kita tinjau dari segi kegunaan *smartphone* sekarang ini tidak dapat dipisahkan dari masyarakat modern global yang cenderung sudah 'kecanduan'. Beberapa fasilitas yang ditawarkan dari produsen *smartphone* yaitu guna memudahkan masyarakat untuk melakukan rutinitas harian baik dari segi pribadi ataupun sosial.

Menurut penelitian yang dilakukan oleh (Purwanegara et al. 2014) mengemukakan bahwa perkembangan saat ini ada peningkatan jumlah pengguna *mobile banking* internet untuk melakukan transaksi di tengah kesibukan masyarakat modern. Teknologi *mobile banking* memungkinkan orang untuk melakukan transaksi kapan saja dan di mana saja. Sehingga perbankan saat ini menawarkan berbagai layanan transaksi secara *mobile* untuk memudahkan para nasabah. Dan penyediaan layanan elektronik *mobile* semacam itu hanya membutuhkan biaya yang relatif lebih murah jika dibandingkan dengan biaya penempatan sebuah mesin ATM (*Automated Teller Machine*) beserta dengan biaya pemeliharaannya.

Pada tahun 2014 Wai-Ming To dan Linda S.L Lai melakukan sebuah penelitian tentang penggunaan layanan *mobile banking* di Cina. Tingginya penggunaan layanan *mobile banking* dan pembayaran secara *online* di Cina didukung oleh pesatnya perkembangan internet dan kemudahan teknologi untuk digunakan dalam membantu kegiatan masyarakat sehari-hari. Bahkan sejak awal tahun 2008 penggunaan internet di Cina telah melampaui Amerika Serikat, yang diproyeksikan sekitar 690 juta total pengguna akses internet di dunia. Pada tahun itu juga merupakan salah satu tahun pemasaran ponsel pintar dengan tingkat besar di dunia, dengan total pengguna *smartphone* diperkirakan sebanyak 451 juta jiwa. Seperti yang tertera pada Gambar 2.1 di bawah ini yang menjelaskan tentang peningkatan penggunaan layanan *mobile banking* dan pembayaran secara *online* di Cina sejak tahun 2010 hingga 2013 (To & Lai 2014).



Gambar 2.1 Tingkat pengguna layanan *mobile banking* dan *mobile payment* di Cina (Sumber : (To & Lai 2014))

Penelitian yang dilakukan oleh Azham Hussain, Hamisu Ibrahim Abubakar dan Norlaily Binti Hashim (2014) tentang mengevaluasi aplikasi *mobile banking* dari segi pengukuran dan sudut pandang penggunaan. Salah satu tolak ukur penentu keberhasilan sebuah aplikasi *mobile banking* adalah kemudahan aplikasi tersebut untuk dapat digunakan (*user friendly*). Serta terdapat empat poin penting dalam menentukan penilaian untuk menilai sebuah aplikasi *mobile banking* yang ditawarkan kepada para penggunanya. Antara lain yaitu efisiensi, efektifitas, aman dan sederhana (tidak menyulitkan) dalam penggunaannya (Hussain et al. 2015).

Meninjau dari ketiga penelitian di atas, peneliti tertarik untuk melakukan studi analisa terhadap aplikasi *mobile banking* karena di Indonesia telah banyak masyarakat yang memanfaatkan fasilitas tersebut. Namun hanya sedikit nasabah yang menyadari perlunya kewaspadaan tentang keamanan dalam bertransaksi menggunakan *mobile banking*. Peneliti bertujuan menganalisa data penting yang terdapat dalam sistem aplikasi *mobile banking*, data yang berpotensi sebagai *vulnerability* tindak kejahatan digital berupa transaksi tanpa diketahui oleh pemilik akun perbankan atau nasabah.

Tahun 2013 Zilole Simate dari Universitas Copperbelt di Kitwe, Zambia, melakukan penelitian mengevaluasi keamanan *mobile network* dalam Kasus Transaksi *Mobile* di Zambia. Dia mengemukakan bahwa dengan memperkenalkan kemudahan fasilitas transaksi *mobile*

banking telah mengubah pola hidup masyarakat modern menjadi lebih dinamis. Namun dari transaksi yang dilakukan dapat terancam oleh adanya tindak kejahatan digital, karena masih kurangnya tingkat keamanan terhadap jaringan GSM yang digunakan. Khususnya jaringan 2G yang masih banyak digunakan di Zambia. Meskipun penggunaan jaringan GSM 3G akan disebar dan cenderung memiliki tingkat keamanan yang lebih baik. Hal ini merupakan salah satu alasan mengapa operator selular harus turut menjaga keamanan jaringan dan mengikuti regulasi keamanan secara internasional. Peneliti mengutip penelitian Zilole Simate karena memiliki kesimpulan bahwa jaringan GSM sebagai jalur internet pendukung fasilitas *mobile banking* telah memiliki sistem keamanan yang dapat membentengi tindak kejahatan digital sebelum pelaku dapat mengakses ke dalam sistem bank (Simate 2013).

Penelitian yang dilakukan Thomas Zefferer dan Peter Teufl (2013) mengenai Penilaian Kebijakan Keamanan Pengguna Perangkat *Mobile* : Sebuah Alternatif Managemen Solusi Perangkat *Mobile* untuk Ponsel Pintar Android, mengkritisi level keamanan dan integritas keamanan perangkat yang digunakan untuk transaksi *mobile*. Banyak para pengguna *smartphone* menonaktifkan fitur keamanan demi kenyamanan, bahkan ada pula pengguna menginstal aplikasi yang tidak terpercaya sehingga tertanam *malware* di perangkat *smartphone*. *Mobile Device Management* (MDM) merupakan solusi dengan menyediakan sarana untuk pengelola aplikasi dan konfigurasi *smartphone*. MDM akan digunakan secara efektif pada layanan *mobile banking* dan *mobile government*, dengan cara bekerja sama sebagai fendor aplikasi pihak ketiga untuk dapat mengintegrasi penggunaan aplikasi yang disematkan ke dalam *smartphone*, serta menjaga fitur keamanan agar tetap aktif digunakan (Zefferer & Teufl 2013).

Penelitian tentang Analisa Potensi Kerentanan Aplikasi *Mobile Banking* yang dilakukan oleh Taenam Cho, Yunki Kim, SungBong Han, dan Seung-Hyun Seo pada tahun 2013 mengemukakan bahwa masyarakat yang menggunakan fasilitas *mobile banking* memiliki tingkat sensitifitas mengenai informasi pribadi yang digunakan dan transaksi keuangan yang dilakukan. Maka peneliti menganalisa penggunaan aplikasi *mobile banking* mengenai hak akses yang tersedia sebagai salah satu mekanisme keamanan di dalam aplikasi tersebut (Cho et al. 2013). Sistem izin hak akses yang ditanamkan pada aplikasi *mobile banking* dapat menyebabkan dampak serius jika level keamanan tersebut diketahui oleh orang lain dan digunakan tidak sesuai pemilik akses yang sebenarnya. Analisa terhadap level keamanan tersebut dapat di lihat pada Tabel 2.1.

Tabel 2.1 Analisa level keamanan yang digunakan Teanam Cho beserta tim

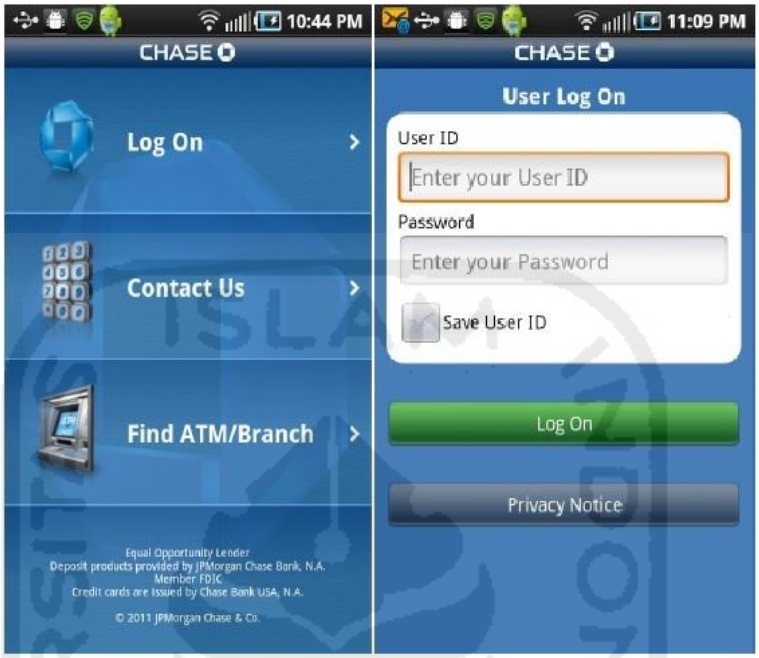
protection Level	**Meaning**
Normal	A lower-risk permission that gives requesting apps access to isolated app-level features, with minimal risk to other apps, the system, or the user.
Dangerous	A higher-risk permission that would give a requesting app access to private user data or control over the device that can negatively impact the user.
Signature	A permission that the system grants only if the requesting app is signed with the same certificate as the app that declared the permission.
System	A permission that the system grants only to apps that are in the Android system.

Peneliti mengutip jurnal penelitian yang dilakukan oleh Teanam Cho beserta tim karena terdapat rencana penggunaan tabel analisa mengenai level keamanan yang terdapat pada sistem aplikasi *mobile banking* yang akan diteliti. Sehingga memudahkan pembaca maupun peneliti selanjutnya untuk mengetahui apa saja level keamanan yang digunakan pada aplikasi *mobile banking* yang diteliti.

Leili Nosrati dan tim (2015) melakukan penelitian tentang Penilaian Keamanan *Mobile Banking* di Iran. Peneliti memandang tindakan *hacking* terhadap akun perbankan secara global (di dunia) telah menyebabkan kerugian yang tak terhitung nilainya. Hal tersebut dikarenakan terdapat banyak kelemahan di dalam sistem perbankan, khususnya peneliti menganalisa sistem keamanan pada aplikasi *mobile banking*. Analisa yang dilakukan bertujuan mengidentifikasi dan mengklasifikasi penyematan sistem keamanan pada *mobile banking.* Hasil yang ditemukan pada penelitian tersebut adalah penggunaan level keamanan berenkripsi, terdapat sistem otentikasi dan otorisasi yang berlapis, serta terdapat sistem keamanan *network layer* (Nosrati 2015).

Penelitian yang dilakukan oleh Biswajit Panja dan rekan-rekan (2013) meneliti tentang analisa keamanan pada aplikasi perbankan *mobile*. Mereka melakukan analisa tentang bagaimana sistem keamanan *mobile banking* dapat diretas untuk mencari informasi tentang akses pengguna dan kata sandinya. Karena pada sistem keamanan jaringan yang digunakan haruslah sudah memenuhi standar kelayakan keamanan. Baik jaringan nirkabel (*wireless*) ataupun jaringan provider GSM. Pada hasil penelitian mengemukakan bahwa sistem keamanan yang diterapkan pada aplikasi *mobile banking* tersebut hanya terdapat pada aktifitas *login* saja, sehingga kemungkinan besar untuk dilakukan tindakan *hacking* terhadap aplikasi masih sangat

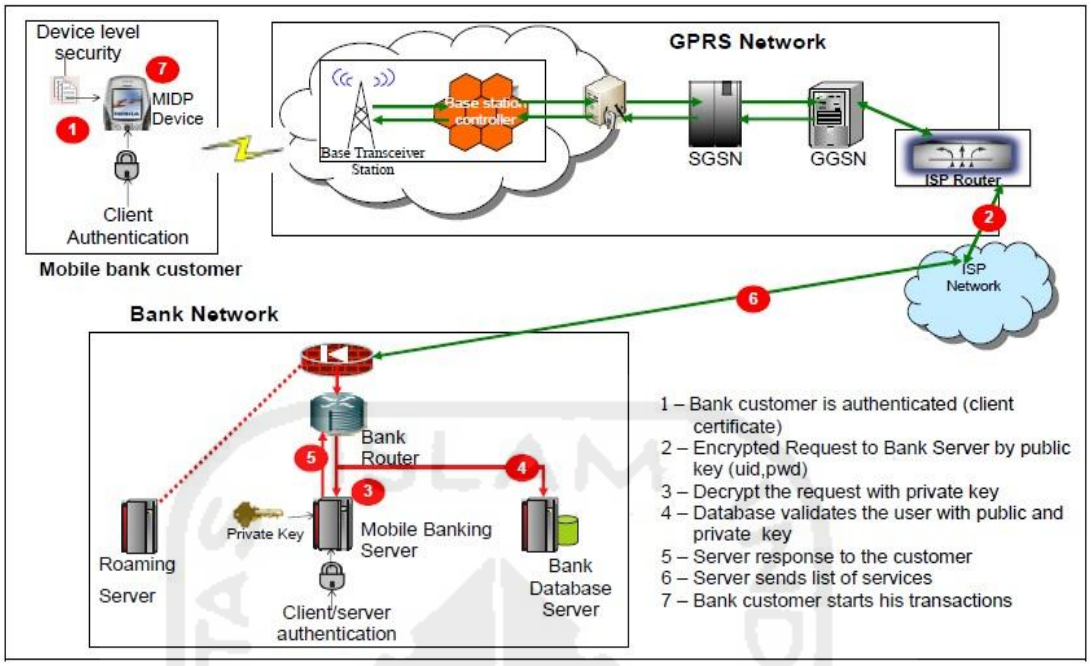
memungkinkan. Pada Gambar 2.2 merupakan tampilan *interface* halaman *login* aplikasi *mobile banking* yang telah dianalisa (Panja et al. 2013).



Gambar 2.2 Halaman *login* aplikasi *mobile banking* yang diteliti
(Sumber : Penelitian C. Narendiran dan tim, 2014)

Penelitian yang dilakukan di India oleh C. Narendiran, S. Albert Rabara dan N. Rajendran (2014) tentang sistem keamanan *mobile banking* yang menggunakan kunci infrastruktur publik, memiliki pendapat bahwa aplikasi *mobile banking* menarik karena nyaman digunakan, meskipun masih terdapat celah keamanan (Narendiran et al. 2009). Kemudian peneliti menganalisa sistem keamanan pada jaringan GSM yang digunakan untuk mengoperasikan aplikasi *mobile banking* yang dimaksud agar dapat terhubung dengan server perbankan. Dan menganalisa apa saja sistem keamanan yang digunakan pada aplikasi *mobile banking*.

Dengan hasil analisa penelitian sistem keamanan yang digunakan dalam proses kinerja aplikasi *mobile banking* tersebut yaitu menggunakan level keamanan pada jaringan GSM yang telah disediakan oleh operator selular berupa kriptografi publik, serta penggunaan tanda tangan digital dan enkripsi pesan yang terdapat di dalam aplikasi. Penjelasan gambaran level keamanan pada jaringan dan *framework* pengoperasian aplikasi *mobile banking* dapat dilihat pada Gambar 2.3.



Gambar 2.3 *Framework* keamanan *mobile banking*

(Sumber : (Narendiran et al. 2009))

Penelitian yang dilakukan oleh Sriramulu Bojjagani dan V. N. Nastry (2015) tentang Protokol Keamanan *Mobile Banking* Berbasis SMS dengan Verifikasi Formal, merupakan sebuah usulan mengenai protokol baru untuk disematkan dalam keamanan aplikasi *mobile banking*. Sistem yang akan ditanamkan pada level otentikasi dan pembayaran ini diharapkan dapat memberikan keamanan dalam komunikasi SMS antara nasabah dengan sistem bank melalui aplikasi *mobile banking*. Metode formal yang dimaksud yaitu berupa *Automated Validation of Internet Security Protocols and Aplications* (AVISPA) dan *Burrows Abadi and Needham logic* (BAN). Hasil yang diperoleh dari penelitian ini adalah meningkatnya level keamanan pada aplikasi dan meminimalisir kemungkinan serangan *hacking* melalui jaringan, karena terdapat skema kriptografi bertingkat di dalamnya (Bojjagani 2015).

Seluruh penelitian terdahulu yang telah dipaparkan telah terangkum dalam *literature review* pada Tabel 2.2.

Tabel 2.2 Tabel *literature review*

No	Nama	Judul	Uraian Singkat	Hasil Penelitian
1	Mustika Purwanegara, Atik Apriningsih, dan Febri Andika (2013)	Snapshot on Indonesia Regulation in Mobile Internet Banking Users Attitudes	Peneliti melakukan survey dan ekplorasi terhadap masyarakat Indonesia yang menggunakan fasilitas *mobile banking* tentang kesadaran mereka dalam menggunakan fasilitas tersebut, memahami regulasi yang berlaku, dan mengetahui seberapa jauh bahaya atau risiko dalam penggunaan *mobile banking*	Para pengguna *mobile banking* di Indonesia secara mayoritas telah mengetahui regulasi mengenai transaksi elektronik. Dan apabila terjadi kerugian material yang menimpa, telah ada payung hukum undang-undang di Indonesia
2	Wai-Ming To dan Linda S.L Lai (2014)	Mobile Banking and Payment in China	Penelitian dilakukan terhadap tingkat penggunaan *mobile banking* di Cina. Peningkatan penggunaan *mobile banking* didukung oleh meningkatnya penggunaan *smartphone* dan akses internet yang mudah didapatkan.	Penyebaran aplikasi *mobile banking* dan pembayaran secara *online* harus diimbangi dengan tingkat keamanan dan kerahasiaan penggunanya. Serta meminimalisir resiko tentang tindak kejahatan yang akan ditimbulkan.
3	Azham Hussain, Hamisu Ibrahim Abubakar dan Norlaily Binti Hashim (2014)	Evaluating Mobile Banking Application: Usability Dimensions and Measurements	Ketertarikan akan penggunaan sebuah produk aplikasi *mobile banking* biasanya bermula dari *interface* yang mudah dipahami. Namun ditinjau pula pada penyesuaian sistem yang selalu dievaluasi terhadap tingkat pelayanan agar selalu nyaman digunakan. Evaluasi tersebut meliputi sejumlah tahapan. Dan yang utama adalah memandang penggunaan *mobile banking* dalam jangka waktu ke depan.	Pengukuran dan sudut pandang penggunaan diyakini sebagai factor kunci keberhasilan bagi penyebaran pemanfaatan piranti lunak *mobile banking*. Bahkan dapat memberikan pelayanan untuk memudahkan nasabah dalam melakukan transaksi kapan pun dan di mana pun tanpa merasakan kesulitan saat menggunakan fasilitas tersebut (*user friendly*).
4	Zilole Simate (2013)	Evaluation of Mobile Network Security A Case of Mobile Transactions in Zambia	Tingginya pengguna fasilitas *mobile banking* di Zambia masih terdapat ancaman tindak kejahatan *cyber*. Karena kurangnya penyematan enkripsi sebagai level keamanan. Serta penggunaan jaringan yang masih pada level 2G.	Pemerintah telah membuat regulasi tentang keamanan terhadap fasilitas transaksi *mobile*. Dan operator selular akan menyebar jaringan 3G yang dapat meminimalisir tindak kejahatan terhadap transaksi *mobile*.

Tabel 2.2 Tabel *literature review* (Lanjutan)

No	Nama	Judul	Uraian Singkat	Hasil Penelitian
5	Thomas Zefferer dan Peter Teufl (2013)	Policy-based Security Assessment of Mobile End-user Devices : An Alternative to Mobile Device Management Solutions for Android Smartphones	Banyak para pengguna *smartphone* menonaktifkan fitur keamanan dengan alasan untuk kenyamanan. Bahkan tidak sedikit pengguna yang menginstal aplikasi tidak terpercaya, karena terdapat kemungkinan tertanam *malware* di dalam *smartphone*. Sehingga keamanannya terancam.	Peneliti melakukan pendekatan kepada fendor aplikasi sebagai pihak ketiga dengan menawarkan MDM (*Mobile Device Management*). Guna mengintegrasi penggunaan aplikasi yang disematkan ke dalam *smartphone*, serta menjaga fitur keamanan agar tetap aktif digunakan.
6	Teanam Cho, Yunki Kim, SungBong Han, dan Seung-Hyun Seo (2013)	Potential Vulnerability Analysis of Mobile Banking Applications	Penggunaan *smartphone* berbasis android membuat tingginya pengguna aplikasi *mobile banking*. Sehingga peneliti melakukan analisa terhadap level keamanan hak akses yang digunakan dalam aplikasi tersebut.	Peneliti mendapatkan informasi tentang level keamanan hak akses yang bertingkat dalam aplikasi *mobile banking* yang dianalisa. Tidak hanya keamanan pada *interface login* saja, melainkan ada keamanan hak akses lagi untuk dapat melakukan transaksi yang diinginkan (misalkan untuk transfer, cek saldo, pembayaran, dll).
7	Leili Nosrati dan Amir Massoud Bidgoli (2015)	Security Assessment of Mobile Banking	Peneliti menganalisa sistem keamanan pada aplikasi *mobile banking* karena terdapat *vulnerability* yang dapat dimanfaatkan oleh *hacker*. Analisa yang dilakukan bertujuan mengidentifikasi dan mengklasifikasi penyematan sistem keamanan pada *mobile banking.*	Hasil yang ditemukan pada penelitian tersebut adalah penggunaan level keamanan berenkripsi, terdapat sistem otentikasi dan otorisasi yang berlapis, serta terdapat sistem keamanan *network layer*.

Tabel 2.2 Tabel *literature review* (Lanjutan)

No	Nama	Judul	Uraian Singkat	Hasil Penelitian
8	Biswajit Panja, Dennis Fattaleh, Mark Mercado, Adam Robinson, dan Priyanka Meharia (2013)	Cybersecurity in Banking and Financial Sector : Security Analysis of a Mobile Banking Application	Peneliti melakukan analisa terhadap aplikasi *mobile banking* mengenai apa saja level keamanan yang digunakan. Karena tidak dapat hanya mengandalkan keamanan pada jaringan saja. Pada aplikasi haruslah terdapat level keamanan yang berlapis.	Pada hasil penelitian mengemukakan bahwa sistem keamanan yang diterapkan pada aplikasi *mobile banking* tersebut hanya terdapat pada aktifitas *login* saja, sehingga kemungkinan besar untuk dilakukan tindakan *hacking* terhadap aplikasi masih sangat memungkinkan.
9	C. Narendiran, S. Albert Rabara dan N. Rajendran (2014)	Public Key Infrastructure For Mobile Banking Security	Peneliti menganalisa sistem keamanan pada jaringan GSM yang digunakan untuk mengoperasikan aplikasi *mobile banking* yang dimaksud agar dapat terhubung dengan server perbankan. Dan menganalisa apa saja sistem keamanan yang digunakan pada aplikasi *mobile banking*.	Aplikasi memanfaatkan sistem keamanan yang berlevel pada jaringan GSM yang telah disediakan oleh provider selular berupa kriptografi publik. Serta penggunaan tanda tangan digital dan enkripsi pesan yang terdapat di dalam aplikasi.
10	Sriramulu Bojjagani dan V. N. Nastry (2015)	SSMBP: A Secure SMS-based Mobile Banking Protocol with Formal Verification	Peneliti mengusulkan protokol keamanan baru berupa Automated Validation of Internet Security Protocols and Aplications (AVISPA) dan Burrows Abadi and Needham logic (BAN).	Hasil yang diperoleh dari penelitian ini adalah meningkatnya level keamanan pada aplikasi dan meminimalisir kemungkinan serangan *hacking* melalui jaringan, karena terdapat skema kriptografi bertingkat di dalamnya.

Berbeda dengan penelitian terdahulu, pada penelitian ini berada pada kategori *Mobile Forensic* dan *Live Forensic* dengan objek penelitian aplikasi *mobile banking* dari perbankan di Indonesia. Paparan singkat mengenai rencana penelitian tertulis pada Tabel 2.3.

Tabel 2.3 Penelitian yang diusulkan

Nama	Judul	Uraian Singkat	Hasil Yang Diharapkan
Adam Prayogo Kuncoro (2017)	Pengembangan Mobile Forensic Pada Aplikasi Mobile Banking Menggunakan Metode Static Forensic	Melakukan analisa dan explorasi terhadap aplikasi *mobile banking* untuk dapat memetakan karakteristik dan fungsi. Mengetahui bagaimana proses pengambilan data dan menggali informasi yang dapat digunakan dalam investigasi tindak kejahatan terhadap layanan *mobile banking*.	1) Melakukan investigasi forensik guna mencari bukti digital terhadap kejahatan terkait layanan *mobile banking*. 2) Mengetahui data apa saja yang dapat digunakan sebagai penunjang bukti digital terhadap layanan *mobile banking*.

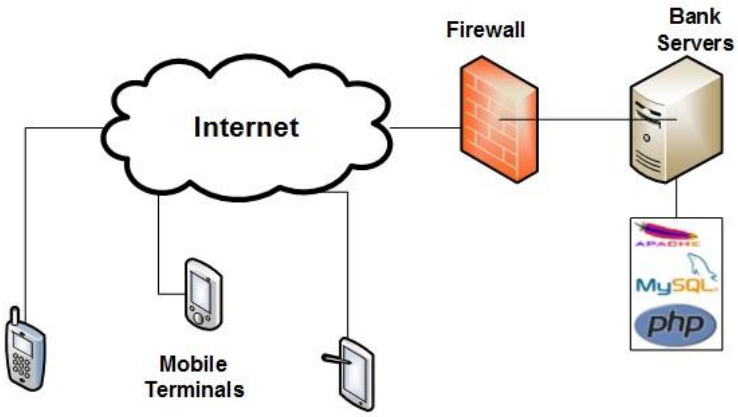
2.2. Landasan Teori

2.2.1. Mobile Banking

Mobile banking merupakan salah satu layanan perbankan yang menerapkan teknologi informasi (Hadi & Novi : 2010). Layanan ini menjadi peluang bagi bank untuk menawarkan nilai tambah kepada pelanggan. *Mobile banking* atau biasa disebut *m-banking* merupakan suatu layanan perbankan yang diberikan oleh pihak bank untuk mendukung kelancaran dan kemudahan kegiatan perbankan. Keefektifan dan keefisienan nasabah untuk melakukan berbagai transaksi *mobile banking* tidak akan berjalan jika tidak didukung oleh telepon seluler dan jaringan internet. Setiap orang yang memiliki *smartphone* dapat memanfaatkan fasilitas ini, untuk bertransaksi di mana saja dan kapan saja dengan mudah. Adanya berbagai kemudahan layanan perbankan tersebut, diharapkan nasabah merasa puas dalam menggunakan berbagai macam jasa yang diberikan oleh pihak bank.

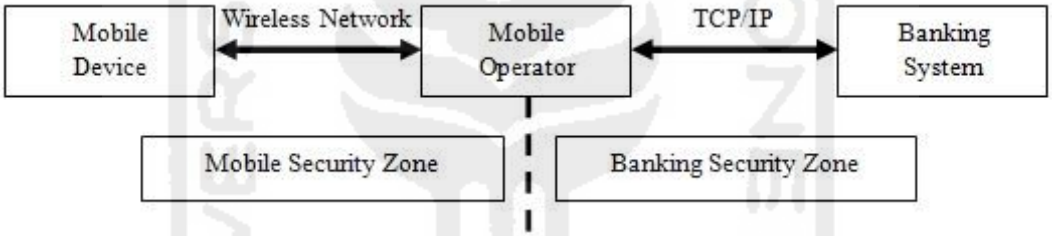
Mobile banking merupakan pengembangan dari sistem *SMS-Banking*. Meskipun sama-sama menggunakan telepon seluler sebagai sarana, *mobile banking* memiliki teknologi yang lebih baru karena menggunakan aplikasi yang harus diunduh dan diinstal ke dalam telepon seluler (*smartphone*), dibandingkan dengan *SMS-banking* yang hanya menggunakan sarana teks melalui SMS. *Mobile banking* adalah salah satu bagian dari *E-banking* yang merupakan layanan informasi perbankan via *wireless* paling baru yang ditawarkan pihak bank dengan menggunakan teknologi *smartphone* untuk mendukung kelancaran dan kemudahan kegiatan transaksi perbankan (Sulistyarini 2012).

Berbagai macam sistem keamanan yang diterapkan ke dalam layanan *mobile banking* baik dari segi perbankan, keamanan berlapis pada aplikasi, bahkan terdapat pula pemanfaatan keamanan pada jaringan yang digunakan untuk terhubung ke internet. Pada Gambar 2.4 merupakan protokol transaksi *mobile banking* secara umum.



Gambar 2.4 Protokol umum transaksi *mobile banking*

Pada Gambar 2.5 berikut ini merupakan contoh pemanfaatan sistem keamanan dari protokol jaringan selular dan keamanan server bank yang terdapat pada transaksi *mobile banking* secara umum.



Gambar 2.5 Bagan pemanfaatan keamanan pada jaringan selular dan server bank

Namun pemanfaatan keamanan dari segi jaringan selular yang digunakan dan sistem keamanan pada server bank tidak dapat mencegah tindak kejahatan pencurian menggunakan aplikasi *mobile banking* jika pelaku dapat menduplikasi hak akses resmi melalui aplikasi. Misalkan pelaku pencurian menggunakan berbagai cara untuk dapat menduplikasi hak akses resmi sehingga sistem keamanan perbankan tidak mengetahui bahwa transaksi yang dilakukan adalah perbuatan pelaku pencurian (tidak resmi), bukan bersumber dari keinginan/tindakan pemilik akun (nasabah) yang resmi. Hal tersebut dapat terjadi, jika pada aplikasi *mobile banking* tersebut tidak dilengkapi dengan sistem keamanan berlipat untuk mencegah atau meminimalisir tindak kejahatan *hacking* atau pencurian menggunakan hak akses yang terduplikasi.

Banyak sistem keamanan yang dapat disematkan ke dalam aplikasi *mobile banking* guna mencegah pengaksesan akun yang bukan bersumber dari pemilik resmi/nasabah. Diantaranya dapat menggunakan keamanan kriptografi, enkripsi, keamanan identifikasi nasabah yang berlapis

dalam setiap akan dilakukannya transaksi menggunakan pin/password yang berbeda-beda (contohnya, seperti pin token fisik pada fasilitas *internet banking*), keamanan pin yang selalu berubah dengan notifikasi SMS dari server perbankan, dan keamanan lainnya. Namun semakin tingginya penerapan sistem keamanan yang berlapis pada aplikasi *mobile banking* sebanding dengan tingginya biaya pembuatan aplikasi atau dalam pemeliharaannya dan pengembangannya. Kembali lagi kepada kebijakan perbankan yang menyediakan fasilitas tersebut untuk tetap memudahkan nasabah dalam bertransaksi tetapi keamanan dan kepercayaan nasabah tetap terjaga.

Dapat pula perbankan melakukan survei terlebih dahulu mengenai tingkat kebutuhan nasabah terhadap fasilitas *mobile banking* sebelum memberikan/me-*launching* aplikasi tersebut. Dengan tujuan untuk mengetahui dan sebagai tolak ukur seberapa pentingnya penerapan keamanan yang berlapis pada aplikasi *mobile banking* yang ditawarkan.

2.2.2. Mobile Forensic

Pada awalnya masyarakat secara awam hanya mengetahui dunia forensika hanya terdapat pada ilmu kedokteran, khususnya di lingkup masyarakat Indonesia. Namun pemahaman dan pembelajaran mengenai dunia forensika saat ini telah merambah ke berbagai aspek yang melekat di kehidupan manusia. Beberapa contoh diantaranya yaitu forensika digital mengulas informasi-informasi penting yang terdapat pada perangkat elektronik digital untuk keperluan tertentu, misalnya informasi yang dapat diperoleh dan digunakan sebagai bukti digital secara sah di hadapan hukum. Ada pula *audio forensic*, *image forensic*, dan lain sebagainya.

Sedangkan ilmu tentang *mobile forensic* merupakan salah satu bagian di dalam ilmu utama *digital forensic*. Pada *mobile forensic* ini adalah ilmu forensika yang berkaitan dengan perangkat-perangkat elektronik yang dapat dibawa ke mana pun secara mudah untuk berpindah tempat (*mobile*). Contohnya telepon seluler, *smartphone*, perangkat GPS, dan lain sebagainya.

Informasi yang dapat digunakan atau yang dapat dianalisa dalam ilmu *mobile forensic* biasanya berupa *history* SMS, *log* panggilan telepon, kontak nomor telepon yang terdapat pada telepon seluler ataupun *smartphone*, *log history* dan informasi penting yang ada di dalam aplikasi *smartphone* guna dijadikan bukti digital, serta berbagai macam informasi lainnya yang berkaitan dengan bukti digital.

Smartphone merupakan sumber dari bukti *forensic*. *Forensic* android adalah bidang di *mobile forensic*, investigasi yang dilakukan berupa pendataan dan analisis data (Walter T. dan Nagoor Meeran, 2015).

2.2.3. Static Forensic

Pada dasarnya proses akuisisi dan investigasi pemecahan kasus yang menggunakan barang bukti digital termasuk ke dalam ilmu *digital forensic*. Terdapat dua pemahaman dasar ilmu mengenai teknik forensika yaitu *live forensic* dan *static forensic*. Tidak ada perbedaan teknik dan metode yang dilakukan antara *live forensic* dengan *static forensic* yaitu identifikasi, penyimpanan, analisa dan presentasi.

Perbedaan pada *live forensic* yaitu analisa yang dilakukan secara *live* atau secara langsung saat perangkat sedang aktif (dalam posisi terhubung ke dalam jaringan). Sedangkan *static forensic* merupakan teknik analisa pada barang bukti secara *off-line*, tidak terhubung ke dalam jaringan dan investigator dapat langsung menangani perangkat barang bukti untuk diakuisisi. Misalnya analisa menggunakan teknik *static forensic* terhadap sebuah *harddisk* dapat langsung dianalisa. Contoh lainnya saat menganalisa perangkat *mobile* (*handphone* atau *smartphone*) dapat dilakukan tanpa terhubung ke dalam jaringan nirkabel.

Forensika tradisional (*static forensic*) dilakukan melalui analisa secara statis, data diawetkan (disimpan melalui proses *cloning* terlebih dahulu) pada media penyimpanan permanen. Tidak semua data diperlukan untuk memahami keadaan (menginvestigasi) dari sistem yang diperiksa (Mrdovic et al. 2009).