論文の内容の要旨

氏名：柏　山　正　守
博士の専攻分野の名称：博士（工学）
論文題名：Pattern Matching Accelerator を用いた車載 IoT Edge 向け
Malware Cyber-Security に関する研究

クルマなどに搭載される IoT(Internet of Things)システムにおいて，潜在的脅威である Malware を自律的に Edge 部分で Real-Time Filtering する手段は，計算コストや消費電力の問題，対応する効果的なアルゴリズムが提案されていないなど多くの課題があり，現在まで，有効性の大きさに比較し，実用化へ向けた研究が推進されることは無かった。しかし，通信でつながるクルマの登場は，車両データの利活用や応用社会実装が進展し，その重要性の高まりとともに Cyber-Security リスクも生まれており，大きなインシデント(Incident)を未然に防ぐ手段を車載 IoT の Edge 部分へ組み入れていく必要性が生じている。

これらの状況への対応策として，Edge 部分にハードウェアセキュリティモジュール(HSM)を組み入れる研究開発が進んでいる。HSM は，ハードウェアとソフトウェアが協調した環境で，TEE(Trusted Execution Environment)や同等の耐セキュリティ機能を内蔵する。しかし，これら機能は，暗号鍵・認証による安全なプログラム実行領域の確保やデータ保護を目的としており，サイバー攻撃(Cyber-Attack)や異常の検出への対応機能を持たない。そのため，Malware 侵入検知機能を追加装備することが必要である。

現在，これら Malware 侵入の検知手段は，高性能な CPU 環境を用いた AI(Artificial Intelligence)活用よる検出手法が一般的である。しかし，複雑な AI 処理を用いた手法は，計算コストの問題から Edge 部でのリアルタイム自律識別処理に限界があった。そこで本提案では，Malware を Texture Image として抽象化し，Pattern Matching Accelerator を用いた多重テクスチャ(Texture)解析を行うことで，IoT の Edge 部分への適用が可能で低い計算コストを実現するシンプルな検出アルゴリズムを創出した。また，計算コスト縮退は，汎用プロセッサに Pattern Matching Accelerator を組み合わせるヘテロジニアスコンピューティング(Heterogeneous Computing)環境を用いることで，非常に低計算コストで Malware Texture Image の全スキャン実行を可能とした。

提案手法は，高次局所自己相関(HLAC: Higher-order Local Auto Correlation)から得られるマスクパターンを用いて Malware Texture Image の構造レベル解析を Pattern Matching Accelerator で行い，パターンマッチングから得られる Malware Texture Image 固有のパワースペクトル特徴量(Power Spectrum Features)を主成分解析するアルゴリズムを用いて Malware 識別を実現した。

提案手法の Malware 識別システムは，80%程度の識別性能を持つ。これらの性能評価は，6 種類の Malware ファミリー群，641 サンプルを用いてエミュレータシステムで確認した。さらに，既往開発結果から導出した計算コスト概算比較では，一つの Malware ファイルの識別処理は，数 100μsec オーダー程度にまで縮退させることが可能である。

提案手法の実証結果より，クルマなどに搭載される IoT システムが求める重要な要件が実現できる。具体的には，Pattern Matching Accelerator の適用と新しい提案アルゴリズムの採用により，Malware 検出を目的とした低消費電力かつ高速処理の車載 Edge 組み込みシステムの実現が可能になる。

本論文は，IoT の Edge 部分において，自律的に Malware 検出を行うアルゴリズムの有効性検証を行い，その方式提案と車載実装について考察を行うものである。

本研究の成果を使うことにより，IoT Edge Computing システムの Malware Cyber-Security を高めることが可能となる。

本研究は，Malware の動的コード解析や静的コード解析などの既往の研究路線とは異なり，Edge デバイスに Malware 検出機能を組み込むのであれば，どのような課題を克服すべきか，という観点で取り組んだ研究である。

既往の解析手法は，いずれも 75%以上の高い識別精度を誇るが，Computing 環境のコストが高いことから Edge への適用は難しい。即ち，IoT Edge Computing へ実装する場合，サーバと Edge とのデータ

交換オーバーヘッドが大きく，リアルタイム性能が劣る。特に，リアルタイムに解析が要求される場合は，Edge の近くに Computing を設けることがセオリーである。重要なファクターは，Edge Computing 部分の計算コストを如何に縮退させるのか，Malware 検出には，どのような機能やアルゴリズムが有用なのか，を探求する必要性が求められる。本論文の提案アルゴリズムは，Edge Computing 部の計算コスト削減に Pattern Matching Accelerator を用い，そのマスクパターンに高次局所自己相関(HLAC)を応用することで，Texture Image という対象物を多段に抽象化し，局所的特徴と大域的特徴を抽出することで，そのものが Primitive に持つ特徴を数値として解析するという新規性のあるロジックを実証したものである。

本論文は 6 章から構成されており，第 1 章では総論として，本研究の全体概要，課題と位置付け，さらに提案の目的と特徴に関して述べる。

第 2 章では，Pattern Matching Accelerator による Malware の構造的解析手法に関して，関係する既往研究手法と導き出される本論の新たなアルゴリズムの着想に関して述べる。本論では，Texture Image 解析と統計量の関係から，Malware の機械語命令列を「大きさや形，配列密度」へ構造的に分類する局所マスクパターンを用いたスキャニングにより機械語命令列の頻出度を導出するアルゴリズへ発展させた。

第 3 章では，提案手法とその Malware 検出アルゴリズムの理論に関して説明する。Malware は，目的を持った固有のコアコードが存在すると仮定し，その機械語命令列の分類を高次局所自己相関特徴(HLAC)マスクパターンで行う構造的解析手法を導出した。具体的には，Malware 機械語命令列の固有コードの規則性から Texture の 1 次統計量(局所)を抽出し，HLAC マスクパターンのマッチング頻度とマスク種類の相関から Texture の 2 次統計量(大局)を抽出する。これら局所と大局の特徴量は，Malware Texture Image が持つ固有のパワースペクトルデータとなり，その固有ベクトル解析を行うことで Malware 識別が可能であると理論付けた。また，提案手法は HLAC マスクパターンによるマッチング頻度の計算処理を Pattern Matching Accelerator を用いることで計算コストを抑え，シンプルかつリアルタイムで行う。

第 4 章では，提案手法を用いた Malware の識別実験に関して，評価手法と実験システムの構成概要を説明する。Malware 識別実測値に対する解析は，ヒストグラムの波形トレンドが，パワースペクトルに類似していることから，モード信頼性評価基準(Modal Assurance Criterion)による固有ベクトル相関確認手法を用いる。さらに，特異値分解(Singular Value Decomposition)を用いた主成分解析により識別率を向上させる。未知の Malware を想定した解析結果より，実験システムと本提案のアルゴリズムは，全体の平均で 79.6%の精度で Malware ファイルの検出が可能であることを実証した(車載システムにおける目標検出精度:70%以上)。さらに，導入した Pattern Matching Accelerator の性能概算より Malware 検出処理時間は 1.1msec 以下，消費電力は 1.4W 以下であると算出した。

第 5 章では，提案手法の有効性と課題に関して，Malware の検知性能を支配する要因と誤検知の割合や難読化 Malware に対する弾性の有無を考察する。さらに，Computing の課題に関しては，既往の識別システムとの計算コスト比較，コンパイラや命令セットアーキテクチャ(ISA)に関して議論する。また，車載実装に関しては，車載 Security Gateway への実装を想定したケーススタディを示す。

最後に第 6 章において，結言と今後に残された課題について述べる。今後に残された課題に関しては，識別性能の劣る一部 Malware 種の解析を推進し，それらに対応する特徴ベクトルのダイナミックな再構築アルゴリズムへの進化研究を進める。さらに，本提案は，異なる命令セットアーキテクチャのバリエーションに対しても有効な汎用識別アルゴリズムであると考えており，これら仮説の実証研究を進めていく。

本研究は Malware Cyber-Security において革新的技術であり注目度も高い。自動車 OEM や自動車部品メーカ，インフラ企業から多数のフィードバックやリクエストを受けており，今後も巧妙化する Malware Cyber 攻撃の最新技術に対応する先進的研究を推進する。