Security Evaluation of Side Channel Attacks on CPS Architectures

[1]Xinhe HOU and [2]Donglai LU
[1]School of Electronic, Information and Electrical Engineering, Shanghai Jiao Tong University, Anhui, China.
[1]xinhehou@gmail.com, [2]dlu@en.ustc.edu.cn

Correspondence should be addressed to Xinhe HOU: xinhehou@gmail.com.

Article Info
Journal of Computing and Natural Science (http://anapub.co.ke/journals/jcns/jcns.html)
Doi: https://doi.org/10.53759/181X/JCNS202101018
Received 24 May 2022; Revised form 20 June 2022; Accepted 26 July 2022.
Available online 05 October 2022.

Abstract – "Smart-Embedded Systems," or Cyber-Physical Systems (CPS), bring together physical, computational, and network resources into a single integrated system. These resources are put to work to provide a solid basis for a better quality of life and a more upscale standard of living. CPSs (Cyber-Physical Systems) are vital in supporting the need for smart products (e.g., airports, homes, cities, hospitals). Control the three sorts of resources Doi: physical, cognitive, and network. In order to uncover the essential knowledge in the various real-life segments, e.g., distribution, power transmission and telecommunication, CPSs stimulates human-to-human interaction via this regulatory measure Information security is a critical concern in today's technological world. Due to the complexity of the components and middleware in CPS, it is difficult to keep them safe from cyberattacks while yet allowing them to operate quickly and effectively. An in-depth explanation of CPS, their issues (including cyber threats), characteristics, and associated technology is provided in this paper Aside from security and performance, we also describe the prevalent Side Channel Attacks (SCA) e.g., Differential Power Analysis (DPA) and Simple Power Analysis (SPA), on cryptographic techniques (such as RSA and AES) and the countermeasures that may be used to protect against these attacks.

Keywords – Cyber-Physical Systems (CPS), Side Channel Attacks (SCA), Differential Power Analysis (DPA), Simple Power Analysis (SPA)

I. INTRODUCTION

Environmental or human-made events may be calculated, interacted with, and managed using CPs, which are embedded networked software programs that were co-engineered by the two parties. High-quality services are provided by the CPSs, which are closely linked. There are a number of distinct systems that make up Cyber-Physical Technologies, including humans, embedded devices, intelligent devices and physical settings. Network elements and communication channels such as the internet help connect everything. Scientific, technological, and societal hurdles still exist for Cyber-Physical Systems. Many diverse physical items and equipment must be integrated with integrated and dispersed systems that must execute the needed duties effectively and according to the standards set in CPS technology. The absence of a common vocabulary and terminology to define cyber-physical interactions is a major obstacle to such integrations. A central link between systems, physical things, and human beings does not exist, making the integration more difficult to achieve interoperability.

One of the most promising new study areas is cyber-physical systems (CPSs), which combine the digital and physical worlds. In order to integrate the physical and digital worlds, these systems use a network of interconnected components that work together to complete tasks. Although CPSs and the Internet of Things (IoT) have made jobs more difficult, they have also made CPSs more scattered, and it is vital to design interoperable CPSs capable of delivering services on time. Distributed real-time multiscale dynamics and interconnection of CPSs is achieved in this way to ensure that the physical domain is monitored and controlled in a trustworthy, safe and secure manner.

When CPSs and IoT are combined, new ideas and methodologies emerge in the creation of CPSs, like service-oriented architecture (SOA), collaborative systems, and cloud computing. When it comes to the interoperability of CPS devices, both on the cyber and physical levels, the results thus far are encouraging for service-oriented CPSs. For global real-time CPSs to be completely realized, a service-oriented architecture alone is insufficient, as this study shows, given the strong interdependencies between virtual and actual components. A distributed ubiquitous computing method based on agents that are aware of their surroundings is thus more attractive since it is possible to include many qualities into agents and achieve greater cooperation and compatibility among autonomously and heterogeneous agents. Sensing, resource finding, adaptability, and augmentation are all made possible by CPSs because of context-awareness. Partial observability in CPSs is a given, given the dynamic nature of dispersed CPSs domains. Uncertainty modeling strategies must be used in order to achieve appropriate model performance when ontologies are used as the underlying semantic technology.

Distributed cognitive systems provide interoperable CPSs that fulfil the demands of virtual and real elements, accordingly. Although most CPS simulation systems are able to model either the physical or the cybernetic elements, they cannot simulate both. CPSs that use service-oriented computing to generate interoperable CPSs have been discussed in [1]. A service-oriented paradigm is not enough to depict multiresolution decentralized CPSs with real-time multiresolution volatility and connectivity in real-time. For distributed complicated systems like CPSs, an agent-based Modeling approach is preferable.

Semantic agent technologies are closely linked to the sensor nodes in CPSs. Using data fusion techniques, a battlefield knowledge factor using semantic agent technologies may dynamically link smart sensors for real-time context-based reasoning. In addition, a service-oriented sensors and data system architecture and programming technique have been given. Data collection, storage, and processing may be made more efficient by using an ontology to abstract information and make it easier to utilize. Software agents that operate on their own initiative may improve the timeliness and concurrency of distributed processing environments farther. Such autonomous semantic agents have therefore been suggested as a new software framework for distributed computing settings.

Since CPSs are highly dynamic systems, semantics and decentralized agents are essential for interoperable CPSs, which must appropriately reflect integrated processing and communication capabilities. Decentralized semantic agent models have been created for CPSs that enhance the data collection process with semantic knowledge. If this approach is selected, it is challenging to think on a local scale concerning the specific components while also focussing on a global scale about the system-range characteristics. Semantics such as these may be used to describe the interactions and observations of system components, even if event identification is needed for distributed CPSs. The semantic agent-centric framework's ontology tends to support certainty logic; hence it requires ways for representing uncertainty in the ontology itself. We have a significant problem in analyzing human-machine interactions and building models that take into account current situational data and environmental changes while interacting with CPSs. Decision-making procedures, particularly in technologies like traffic control and weapons technology, must be improved. Moreover, in complex CPSs, where suspicious activity must be dealt with swiftly using machine learning methodologies, the results and responses must not be unexpected or ambiguous. Existing methods for identifying suspicion are still minuscule; software design flaws, network connectivity issues and faulty physical items worsen the issue.

As a result, it's difficult to maintain the same level of precision, durability, and performance throughout all system components. In addition, there are issues with the design phase of such networks, as well as issues with comprehensibility and modifiability. Modern technology is, as always, built on three pillars: security, privacy, and trust. Reliability and security of a CPS are challenging to maintain from a technical and political standpoint, as is the protection of the personal information contained within. Infrastructure, workers, intellectual property, and goods are all safeguarded by many levels of CPS security. It is crucial to balance the need for early detection of cyber and physical concerns with the need for security that can be guaranteed while also maintaining the necessary performance. Protecting sensitive and confidential information in CPSs often calls for determining the system's optimum performance while also taking privacy and security concerns into account. The required levels of security, privacy, and operation of the system for each CPS are all updated as due to this to provide the greatest results.

This paper provides a basis of understanding regarding the features and associated technologies of CPSs as well as the issues they face (including cyber-security assaults). As part of our research, we look at how cryptographic algorithms (such as asymmetric RSA and symmetric AES) are vulnerable to Side Channel Attacks e.g., Differential Power Analysis (DPA) and Simple Power Analysis (SPA) as well as the countermeasures that may be taken to protect against them. The remaining part of the paper is organized as follows: Section II presents a background analysis of the research. Section III reviews the cyber security attacks. Section IV reviews the relevant sources of literature related to the research. Section V focusses on the security and safety objectives of CPSs. Section VI provides a critical analysis of SCAs and the available countermeasures; while Section VII concludes the paper.

II. BACKGROUND ANALYSIS

A Cyber-Physical System

A computer-based technique is used to regulate or monitor a process in a Cyber-Physical System (CPS). Because of the complex interplay between hardware and software components, it's critical that we understand the many spatial and temporal dimensions at which these systems operate as well as how their interactions change with the surrounding environment. "Cyber-mechatronics" and "process science" are all included in CPS, which uses a multidisciplinary approach. Embedded systems are used to refer to the control of the manufacturing process. An intensive relationship between computational and physical parts is less common in embedded systems. Rather, focus is on the computational elements. CPS, in contrast to the Internet of Things (IoT), combines and coordinates physical and computational components in a more complicated manner. Control and guidance systems for automated pilot avionics may be a part of CPS in addition to smart grids and autonomous cars. CPSs could be noticed in various segments e.g., diverse as aircraft, automobiles, industrial processing, infrastructure, power, health care, manufacturing, and transportation, as well as leisure and home appliances.

Physical input and output are common features of full-fledged CPS systems, unlike more ordinary embedded systems. Computational intelligence methods are at the forefront of this concept, which is deeply rooted in robotics and sensor network concepts. Progress in engineering and science has made it easier to connect physical parts to computer systems through intelligent processes, boosting the system's scalability and flexibility as well as its efficiency, functionality and dependability. Cyber-physical systems will be able to do more in a variety of directions, including: intervention (for example, collision avoidance); accuracy (for example, nano-level manufacturing and robotics surgery); operations in vulnerable and inaccessible domains (for instance, searches and recoveries; deep sea explorations; and firefighting); cooperation; potency; and modernization of human capacity (for example, zero-net energy structures); and so on (e.g., in healthcare delivery and monitoring).

Sensor-based communication-enabled autonomously systems are the most common use cases of CPS. In several sensor networks, for instance, the data is sent to a central node after being processed by sensors. Autonomous vehicles and medical monitoring are only two examples of CPS that may be used in other industries as well. The MIT Distributed Robot Garden, where a group of robotics tends a yard of plants, is an example of this kind of technology in action. This system integrates decentralized sensing (each plant has a sensor node assessing its state), navigation, manipulating and wireless connectivity. Resilient control systems are being researched by the Idaho National Institute and its colleagues, with an emphasis on control system components of CPS. A more holistic approach to next-generation design is used in this endeavour, which takes into account elements of resilience that are difficult to quantify, e.g., human interventions, intricate interdependency and cyber security.

CarTel, MIT's continuing taxi-gathering initiative, is another example of how technology is being used to improve public transportation in the Boston region. This data is then combined with previous records to determine the most efficient routes at a certain time of day. Also in the smart grid context, CPS are employed in electric grids to conduct enhanced control in order to integrate distributed renewable power more effectively. When wind farm production is too high, a specialized corrective action plan is required to keep the grid's current flows under control. This sort of problem is best addressed by using a distributed CPS. Cloud-enabled cyber-physical systems have led to new techniques in industry. For example, the European Commission's IMC-AESOP project, which included the likes of Schneider Electric, SAP, Honeywell, Microsoft, and others, highlighted the way to Industry 4.0.

Side Channel Attacks (SCA)

A SCA is an attack against the personal data of a cryptographic device. In the SCA realm, the phrase 'data' generally refers to the private key of a cryptographic technique. For each LWC cipher, the most recent hardware and software versions are chosen, with an emphasis on the cipher's unique qualities, and both methodologies are extensively evaluated. For example, in [2], while the authors present a number of ways for developing lightweight implementations of common algorithms, they also highlight the core components that must be incorporated in programmes and the primary restrictions that the approaches should address. More than a dozen unique variants of SCA have been observed in research. The most common types of attacks include timing attacks, fault attacks, and security analysis attacks.

Simple Power Analysis (SPA)

A SCA known as the “Simple Power Analysis” (SPA) analyses a chip's current utilization over time. It is easy to tell what sort of activity is being conducted at any given moment because various operations have distinct power profile. The amount of current used, for example, may distinguish between an addition and a multiplication function. It's also worth mentioning that the power profile will show the ratio of one to zeros while reading data from a storage device. A typical oscilloscope may be used to collect the resulting current signature and ascertain the operation type.

Differential Power Analysis attack (DPA)

Another sort of SCA that has been examined in this study is Differential Power Analysis (DPA). Unpredictability in power use may be used to find hidden information. Inconsistencies in power use may be due to a plethora of data-driven calculations and processes. This attack relies on both data collection and data processing. Below is a study of DPA attacks as well as countermeasures for AES and RSA. Data-driven analysis (DPA) is a quantitative tool for studying power use. This method is used to determine the variance between the mean trails of two data sets. There is no correlation between the two if the variance is very small. There will be a distinction between them if the sets are linked. If you have a high enough number of traces to average over, there is no limit to how much noise you can detect in a data collection.

Countermeasures

The use of effective and low-cost cryptographic implementation of encryption techniques may aid in the prevention of these attacks. DPA and RPA/ZPA are being disrupted using a Binary Expansion algorithm with a random starting point. To avoid MESD and ZESD, it was suggested that message masking prior to multiplications be done with a randomized value (r) and that exponent masking be used to prevent SEMD.

III. CYBER SECURITY ATTACKS

In order to apply key management strategies implicitly due to security concerns, the Internet of Things provides a distinct field called the key identifier module. Digital certificate keys, group keys, pair keys, and single keys may all be used in the field simultaneously. You will find the source and index keys in this field. Second, the key index is used to maintain track of the unique identification of all keys that have a common origin. The first element, key source, describes the key's origin. Maintaining the secrecy, integrity, and validity of the encryption keys might be a challenge when it comes to encrypting data. The process of revoking and upgrading keys for nodes that have been hacked or found to be malicious may also be defined as part of key management. Public/private key pairs, private keys, non-secret parameters, initialization variables and supporting key management may all be included in the contents of a key in different instances.

Open-source software is not just a hindrance but also an issue for the Internet of Things (IoT). It is possible for anybody to use this application, making it possible for them to publish and download new tools without the need for further authorization. As a result, developers working on open-source projects like the Internet of Things may benefit from secure key management. In MANETs, nodes that function as hosts and routers are self-governed. These nodes are wirelessly connected in order to sustain one another. A single-hop communication occurs when the sender and receiver are in close proximity; a multi-hop transmission occurs when the sender and receiver are not in close proximity. It is challenging to maintain keys in MANETs because there is no centralized control, devices are mobile, and resources are limited. Because of the limited capabilities of sensors, processors, and nodes, wireless sensor networks (WSNs) are unable to process, store, transmit, or consume battery power to their fullest potential. The broadcast and uncontrolled nature of WSN nodes makes cryptographic key management a huge challenge. Symmetric cryptography is often not an appealing choice for WSNs because of their restricted scalability and the demand for battery and processor resources. The computational and energy footprint of asymmetric cryptography, in contrast, is large, making it less enticing.

With a large network with a lot of IT devices, users more likely to be vulnerable to side-channel attacks (**Table 1** outlines the most prevalent forms of side-channel assaults). It is difficult to apply security and encryption measures on sensors because of the limited processing capabilities, making it difficult to prevent data from being obtained by unwanted parties and to keep personal information safe.

Table 1. Common types of side channel attacks

Attack	Description
Cached side-channel attacks	Monitoring operations such as AES T-table entry, module coefficients or multiplication, or memory accesses may be accomplished by a caching side-channel attack. Attackers may determine an encryption key from the activities of victims, based on the accesses (or lack thereof) they make (or lack thereof). Unlike previous side-channel threats, this method does not interfere with the existing cryptographic mechanism and is fully undetected to the user. Two CPU vulnerabilities (called Meltdown and Specter) were discovered in 2017 that might allow an adversary to leak data from the memory of other applications and even the operating system itself through a cache-based side channel.
Timing attacks	When the cryptographic algorithm or program is being executed on hardware, a timing attack keeps an eye on data moving in and out of the CPU or memory. It's feasible to deduce the complete secret key only by keeping track of how long different cryptographic procedures take. Statistical analysis of time measures is required for these attacks, and they have been shown across a variety of network topologies.
Power-analysis attack	More data may be gained by monitoring the power usage of hardware devices, such as CPUs or cryptographic circuits, using power analysis attacks. DPA and SPA are two subcategories under which these assaults fall. This is an example of how machine learning works Radio waves are also generated as a result of fluctuations in current, making electromagnetic (EM) emissions measurements easier to attack. Similar statistical approaches are used in these assaults as in power-analysis cyberattacks.
DL-based side-channel attack	Deep Learning (DL) side-channel attacks have been shown capable of cracking the private key of a different but comparable device in as little as a single trace on distinct but similar devices. There are analogues for today's side-channel attacks throughout history. On an oscillator, a Bell telephone technician in 1943 saw spikes that might be linked to the decoded output of an encrypted teletype, according to newly disclosed NSA documents. An ex-MI5 officer has claimed that MI5 employed cipher technologies in the 1960s to investigate its outputs for intelligence reasons, according to Peter Wright. IBM Selectric typesetting machines created electromagnetic noise when the type ball spun and pitched to touch the paper; the idiosyncrasies of those signals may disclose which key was pressed. This was hypothesized about by Soviet eavesdropping in the 1990s.

When it comes to symmetric-key algorithm standards, AES is the most extensively utilized. Rijndael was originally known as Rijndael, but after being selected as a contender for AES owing to its advantages, it became a popular method. In several applications, it is relied upon by hundreds and thousands of people all over the globe. AES was thought to be secure until researchers revealed that side-channel assaults (SCA) were effective in breaching its security. SCAs like power analytics and EM (electromagnetic analysis) have made it possible for researchers to begin experimenting with new methods for developing countermeasures. Researchers describe in great depth the features and associated technologies of CPSs as well as the issues they face (including cyber-security assaults). As part of our research, we look at how cryptographic algorithms (such as symmetric AES and asymmetric RSA) are vulnerable to Side Channel Attacks, as well as the countermeasures that may be taken to protect against them.

IV. LITERATURE REVIEW

Due of CPS technology's high significance for networking and data technologies research, the American president was first presented with its findings in 2011. Since then, CPS-related technologies, difficulties, and possibilities have been examined by academics, and their models and applications have grown significantly. This technology faces a major challenge: the CPS safety and security-performance trade-off. An important worry is enabling secure communication and protecting against the propagation of untruthful data, as the current security solutions do not adequately address this kind of system's unique requirements. If no ideal balance among performance and security is explored during CPS design, serious losses may also arise. Though security in CPS is an issue that needs to be addressed, there are still insufficient efforts to do so, and all of the solutions studied so far are based on current security techniques.

We will take a look at a few of the studies that have looked at the trade-off between security and performance in CPS systems. It is possible to improve CPS's security-to-performance ratio. Using the Co-evolutionary Genetic Algorithm (CGA), they were able to achieve effective optimization outcomes. Security and safety necessities conflict with other CPS domain necessities such as performance. System cost estimates and security requirements are used to propose an optimization process for performance-privacy balance. In any networked computing platform, it is known that it is difficult to maintain good security without degrading performance.

Security has received more attention than performance in a number of research studies; these studies have only looked at security as a stand-alone issue. The authors of [3] discuss the security challenges faced by CPS, as well as possible threats and attacks, as well as specific characteristics that set CPS protection techniques apart from those of traditional IT processes. New adversary designs for CPS are also an important topic of discussion in this article. In [4], several common aspects of CPSs are discussed, including their surroundings, real-time needs, uncertainty, and geographic dispersion. It is recommended that developing appropriate security tools for CPSs at the very start of the architecture phase is important in addressing security concerns. Security is an important aspect of the CPS development process, and it should be taken into consideration from the beginning of CPS design. Safety for such systems can be improved by utilizing three different but complementary methods. These methods include methods for protecting multi-domain designing and simulation, methods for increasing attack resilience, and procedures for identifying potential threats to the computer hardware itself.

Control networks, data systems, and networks are now tightly integrated in contemporary control systems. The notion of a Cyber-Physical System (CPS) has been proposed to explore different cyber-attacks in this kind of system. CPS is a network-based intelligent system that integrates and interacts with both computational units and physical things. Data analysis and dynamic processes go hand in hand, which makes it especially sensitive to data transmission mistakes or assaults like denial of service (DoS). The Brazilian power system failures and the shockwaves caused by an Iranian viral assault are only two examples of how this might lead to significant losses or harm. In recent years, the scientific world has paid close attention to the topic of CPS security.

A wide range of assaults may be inserted into CPSs in a stealthy and unanticipated manner because of the systems' vulnerability. These two categories of publications focus on data physical security system, which is currently being researched. The first category focuses only on preventing assaults. There has not been enough investigation on how to accurately estimate the secure state and regulate CPSs in the existing studies. It is still a pressing issue to figure out how to accurately estimate and regulate the condition of a system in the face of an assault

Control theory relies heavily on state estimate. With this strategy, you can better understand and regulate a particular system's dynamic properties than you could with the previous way. State estimate is especially significant when the condition of the system cannot be determined directly. It is possible to tackle the difficulty of state estimate by creating a suitable observer. A state reconstructor is a term that describes a chaotic system depending on the real values of the system's exogenous factors (input and output). Similar to a reference generator, but with a different range of applications. Circuit creation is the primary function of the reference generator.

Collaborative estimation of the status of an LTI system controlled by a network of devices (nodes) was investigated in by Chen [5]. After a sensor or actuator was damaged, the researchers investigated how linear systems may be estimated and controlled in the absence of such components. Estimation of the safety status is presented using an algorithm. Additionally, a set of algorithms developed by Oluwafolake and Solomon [6] may identify fraudulent data opportunists in large-power process model. A drawback of the algorithmic approach described above is that it cannot ensure accuracy, while the observer-based strategy responds quickly and conserves computational resources. Xiao [7] recommended a new state observer. For measuring the security condition of physical networks, Power [8] explored the problem and introduced a new security Luenberger observer. King and Phipps [9]explicitly states that only exponential descent or a large enough step to reach the security state approximation is permitted. This might take a long time. In order for this to operate, a finite-time estimate is required. As a result, even though many authors developed the notions of elastic reliability index and system sparse index, they did not consider the actuator attack while developing their finite-time state observer. A finite-time state estimation under actuator assault may be studied. Security state estimate for CPSs is important, but a variety of security management measures must be explored to minimize the impact of assaults. It is not uncommon to see new studies on CPS controls, such as [10] being published. Design approaches like linear feedback, slipping mode management, elastomeric regulate, and T-S fuzzy regulation have all been touted as very successful and innovative.

Ivanov and Raykov [11] proposed a distributed controller approach for stochastic network attacks and established the system's stability that use the Lyapunov function. A continuous-time controller that is dependent on the observer was presented in [12] to solve the issue of system dependability control. Adaptive resilience may be strengthened to withstand aggressive attacks. Dhaouadi and Kubo [13] also used industrial 4.0 to tackle elastic nonlinear control problems. Systematic design technique for dynamical Event-Triggered Control (ETC) systems under DoS attacks was described by

Wildhagen, Dürr and Allgöwer [14]. In the reference, it was proposed that adaptive event triggers may be based on the failure of random sensors. Since CPSs' network capabilities are limited in the combination of computational, networked, and physical approaches, most prior investigations have focused on coordinated management rather than event-triggered control. Event-triggered control is crucial for investigating destructive assaults on CPSs. Event-triggered control for CPSs was examined by Ma, Che and Deng [15], but malicious attacks were not considered.

There are a variety of device and software-specific LWC ciphers that may be used in a variety of settings. The most modern hardware and software variations for each LWC cipher are selected, with a focus on each cipher's specific properties, and both techniques are thoroughly examined for each cipher. Schaller, Hellmuth and Stadler [16] underline the essential aspects that should be integrated into the programs and the primary limitations that the strategies should address, including how to describe a number of ways for building lightweight designs of common algorithms.

V. SECURITY AND SAFETY OBJECTIVES IN CPS

One of the reasons for the fast growth of CPS is the increasing attention that CPS has gotten over the last several decades in the fields of computing and communication. Smart grid, healthcare and water/gas transmission and industrial operations control are just a few of the industries where this technology has been extensively used. For example, Safety-Critical Cyber-Physical System (SCCPS) are commonly utilized in industries that have a direct impact on the economy and people's lives such as aircraft, nuclear power, public transit, financial services, and healthcare. There will be grave danger to human life and property if the system's implementation goes wrong. As a result, safety and dependability of safety-critical technologies must be thoroughly examined and verified throughout the design and construction phase. Indeed, it has received a lot of attention from scholars and has become a major study issue in the society. To put it another way, SCCPS is a hybrid cyber-physical system. Constantly changing physical behavior and discretely changing decision management behavior are interwoven in these systems. Infinite state areas are also available to them. SCCPS safety assessment and validation become more complicated and pose serious issues as a result. It is, however, difficult to adequately verify classical model checking because of the issue of space vector explosion.

To estimate the chance that the target system matches the sequential logic properties and can give arbitrarily tiny error limitations, statistical model checking (SMC) utilizes statistical analysis methods with the execution route of the sampling system. As a result of SMC's lack of requirement to examine the complicated logic within target systems, it may successfully prevent the system complexity and the growth of state space. As a result, SMC is the best method for determining the timing characteristics of complicated SCCPS. For SCCPS demanding exceptionally high safety, the chance of occurrence of negative occurrences of its safety qualities and the frequency of equipment failures is extremely low. SMC is unable to sample events with a low likelihood of occurring. SMC verification of the ultra-secure SCCPS is a pressing issue that must be addressed as soon as possible.

The significance sampling approach has been the primary way for verifying the SMC's unusual qualities to date. Zhang, Gao and Yu [17] used heuristic approaches to complete the attribute verification of CTMC and DTMC random models, respectively. Cross-entropy reduction critical sampling was developed by Uribe, Papaioannou, Marzouk and Straub [18] as a way to ensure model safety. Hamdan and Mahmoud [19] employed the SMC approach to test the discrete-time SHS' secure characteristic. It is assumed that the system path space has an exponential distribution in the approaches provided by the authors An important sampling distribution may be calculated by raising system parameters' failure rate to extract numerous pathways that fulfill the unusual qualities at one time. It was found that Li and Tam [20] used the cross-entropy minimum iterative algorithm, which increases the number of commands (parameters) in order to get a priority probability density for a random guardian command structure. In contrast to the system route space distribution family, the optimum significance sampling distribution derived by these approaches is basically a heuristic sampling method. As a consequence, the findings of the verification are just approximate.

CPS provides numerous avenues for malicious actors to launch attacks because of its unprecedented ability to connect physically integrated physical power stations and cyber aspects. It is harder to execute physical isolation due to the increased risks that are introduced by next-generation information technology applications like big data, cloud computing and the IoT. There are two primary security concerns in CPS: how to ensure safe operation and how to maintain control performance under attack. The transfer of data via a heterogeneous network has really allowed CPS to achieve higher-complexity and higher-risk industrial process control. CPS control systems may be threatened by malevolent cyber-attacks since open communication networks are major components of societal safety-critical infrastructure, which are vulnerable to such assaults. The incidence of cyber-attacks on power infrastructure has been steadily rising throughout the globe. There was a cyber assault on a power plant in Ukraine, which resulted in a blackout that affected 225,000 people. In addition, the "Stuxnet" malware, a powerful computer worm, infiltrated Iran's nuclear complex and did extensive damage. These findings suggest that the malevolent network in CPS is causing major economic losses and severe social harm, which has drawn the attention of many experts.

Deceptive assaults, fake data injection attacks, and denial-of-service attacks (DoS attacks) are the most common types of network threats in CPS. DoS attacks, a more accessible attack technique, hinder the adversary from exchanging information whereas the fake data injection attack alters the data integrity of a packet by manipulating its payload. A denial-of-service attack (DoS) prevents wireless networks from updating their data in a timely and full manner by interfering with the measurement status or control signal transmission. As a result, a denial-of-service attack aims to degrade system performance to the point of instability. During DDoS assaults, packet dropouts are a common occurrence. It is important to remember that data may be sent as a "packet," which means that a series of control predictions can be sent in a single data transmission and then selected to compensate for packet dropouts based on the current network status.

There have been a variety of measures made to regulate security in the face of denial-of-service (DoS) assaults. Some of the studies examined the impact of network delays. There are several techniques for dealing with the problem of delay. Some additional studies [21] reveal that a wide variety of measures have been tried to mitigate the negative effects of packet dropouts. There is a defense technique offered to cope with the flow of information between the sensors and controllers that congests the communication signal against DoS assaults on the multichannel CPS. Due to the limited capacity of the network, certain scheduling methods are developed in order to maintain communication security whenever control plants have access at each sampling moment. The packet dropout at a lower sampling bandwidth must be addressed if an efficient scheduling algorithm is not included in the CPS design. In other words, it not only makes sure that the system can be scheduled but also assures that the CPS is stable in general.

If the packet dropout rate is related to closed-loop stability analysis, then a schedule algorithm which is based on that relationship should be developed. Then, controllers should be designed to achieve closed-loop system stability using the appropriate methods. Stochastic systems and switching system methods, for example, are useful ways to deal with model and control concerns with packet dropout. Modeling the network infrastructure as a switch and proposing the design control approach of state feedback for systems with arbitrary and limited packet loss] uses the observed output data to create a token-dependent static feedback SMC. The security management is set up to combat assaults that cause substantial packet dropout since it only considers attacks on the backward links. There are viable attack patterns and status feedbacks controllers that can handle both-side communications with random packet dropouts generated by assaults.

Table 2: Security and Safety Objectives in CPS

Objective	Details
Confidentiality	Any unauthorized person or entity, whether within or outside the system, cannot access confidential data and information. Encryption methods are used to protect stored and transferred data, and data storage locations are locked down to prevent unauthorized access. Channels of communication are protected against eavesdropping in CPS to avoid the system state being determined, which may arise due to eavesdropping, from being discovered.
Integrity	In other words, integrity is the capacity to preserve data in its original form and to preclude any illegal alteration of it. Furthermore, the data should be protected from both external and internal tampering. Consequently, an endpoint will receive false data and proceed as if it were accurate. This ensures that CPS's physical objectives and sensor data are not tampered with, and that the authenticity of the CPS's data are maintained.
Availability	System responsiveness is a measure of how quickly the system responds to user requests and produces useful results. Accessibility is the capability of all subsystems to perform correctly and do their task on time and when necessary. The integrity of CPS subsystems is ensured through the prevention of all forms of corruption, including hardware/software breakdowns, power outages, as well as denial-of-service (DoS) assaults.
Authenticity	There must be a way to ensure that all parties involved in CPS proceedings are doing so. To have a true CPS, integrity must be achieved across all components and operations.
Robustness	Robustness refers to how well CPS continues to function despite minor disruptions. When something goes wrong, it may either be a little setback or a major setback with long-term ramifications.
Trustworthiness	Humans (e.g., Proprietors, clients, and persons) may depend on the CPS to fulfill needed activities under specified domain limitations and certain temporal circumstances. Trustworthiness For a CPS to be considered viable and dependable, it must have high levels of dependability in its application, equipment, and data.

VI. SIDE CHANNEL ATTACKS AND COUNTERMEASURES

Zhang and Fan [22] was the first to propose the Side Channel Attacks (SCAs). Hardware-based cryptosystems are vulnerable to attack because of leaked information about the power consumption and system performance of the processors. The SCA aims to disclose the private key and could be used to numerous operating cryptographic gadgets such as smart chips, cell phones, RFID-based networks and CPS. Its purpose is to reveal the secrets.

A SCA is a kind of assault against a cryptographic device's personal data. The term 'data' in the domain of SCA often refers to a cryptographic algorithm's private key. The most modern hardware and software variations for each LWC cipher are selected, with a focus on each cipher's specific properties, and both techniques are thoroughly examined for each cipher. They also underline the essential aspects that should be integrated into the programs and the primary limitations that the strategies should address. More than a dozen distinct forms of SCA have been documented in studies, according to Liu, Zhao, Wang, Guo, Zhang and Ji [23]. Timing assaults, fault assaults and security analysis assaults are among the most frequent. Here, we'll be focusing on a power analytics attack, which uses power usage data to figure out where information is being leaked.

A wide range of approaches, from the intrusive (such as microprobing) to the noninvasive (such as cryptoanalysis), are at hackers' disposal for breaking into a system and stealing confidential data. To get access the data on a chip, a side-channel assault employing power analysis is one of the most straightforward and successful methods. Using power analysis to extract the information of a microchip or smartcard without mechanically de-processing the device is a low-cost and efficient method. It is possible to deduce the contents of a gadget by analyzing the variance in power usage. Both the Simple Power Analysis (SPA) and the Differential Power Analysis (DPA) are methods for analyzing electrical energy levels in a system.

Simple Power Analysis (SPA)

A SCA that evaluates a chip's current usage over a time is known as Simple Power Analysis (SPA). One can tell what sort of operation is being carried out at any given moment since various operations have distinct power profiles. One may discern between an addition and a multiplication function based on the amount of current they use, for example It's also worth noting that while reading the data from a storage, the power profile will represent the ratio of one to zeros. The resultant current signature may be captured and used to determine the operation type using a conventional oscilloscope.

Differential Power Analysis attack (DPA)

Differential Power Analysis (DPA) is another type of SCAs that has been evaluated in this paper. Hidden information may be uncovered by utilizing the unpredictability in power usage. A multitude of computations and procedures based on data may be to blame for power use inconsistencies. Both data gathering and data processing are key components of this attack. The analysis of DPA attacks and the countermeasures for AES and RSA are provided below.

Power consumption data may be analyzed using a statistical approach called differential power analysis. The difference between the average of the traces of two sets of data is computed using this method. Close to zero difference means there's no correlation. The difference will be greater than zero if the sets are correlated. There's no limit to how much noise you can notice in a data set if you have a large enough number of traces to average across.

An attacker may use fault analysis to interpret ciphertext and extract tokens by introducing or exploiting bugs within a system. Errors are most often caused by voltage fluctuations, timekeeping errors, or radiation sources other than the intended one. To perform the attacks, an attacker encrypts a bit of data twice and compares the two encrypted versions. This indicates that there is an issue with one of the processes. A fast computation may now be performed to identify a round in which the error occurred, for example, for DES. There are now a number of steps that can be taken to retrieve the previous round's DES sub-key. There are only 256 ways an attacker can estimate the omitted binary number (the sub-key utilizes 48 bits), or he can peel off last round for which he understands the sub-key and intrusion the diminished DES. Both options are possible when this sub-key is known. Using this method against Triple-DES is also an option. [24] provides a detailed account of the assault. Other methodologies, such as differential-key attacks or disparity corresponding key cryptanalysis, are used in tandem with DFA to gain an advantage. In order to acquire symmetric encryption, a different type of error detection is used: Non-Differential Fault Analysis (NDFA) (such as of DES). Using instinctually broken components (that have been misfiring since manufacturing) rather than tampering with them is an important feature of these attacks because they don't require accurate encrypted messages (i.e., ciphertexts established before the component was compromised).

It is the modular reduction that is targeted prior to modular exponentiations in the DPA assault on CRT-RSA for RSA systems. A correlation attack on a random subset of RSA communication energy use traces is used to find the prime. Correlation attacks that exploit a link between sequential modular quadratic formula procedures and modular mathematical calculations were introduced in [25]. An attacker may introduce a user-defined text into RSA and disclose the private key with less energy usage trace quantities than is required by DPA, according to CPA. X (div N) & X (div N) were used in a separate assault in [26]. This technique was modified to incorporate various sorts of collisions by establishing an energy usage trace collisions based on the Z & Y signal pairs, which meet the Y, Z (div N) pair. SAED (Subtraction Algorithm Evaluation on Equidistant Data) is a new DPA attack introduced in [27]. Due to their presumption that equal distance input will lead to algorithmic changes affecting the energy signal, this threat does not account for differences in the used power level and avoids it. Subtraction event data is being used in the threat to obtain the secret data that is relevant.

Countermeasures

Countermeasures against side-channel assaults come into two broad categories: those that prevent the leakage of information and those that prevent the leakage of information. Reduce or eliminate the disclosure of such information, as well as the link between the disclosed data and secret data. When a cryptographic operation (e.g., deciphering) affects data in a way that may be undone, this is what's often used: an unpredictable encrypted output. There are currently screens on the market that are shielded from electromagnetic radiation, making them less susceptible to TEMPEST assaults. These methods may help protect against power monitoring attacks, but they must be utilized judiciously since even the smallest correlations can jeopardize security. Enclosures may limit the danger of microphones (to protect against acoustic assaults) and other micro-monitoring sensors being installed in an undetected manner (against CPU thermal-imaging and power-draw attacks).

The use of noise to obstruct the emitted channels is yet another countermeasure (also in the first category). Random delays may be inserted to ward against timing assaults; however, adversaries can adjust by averaging many measurements in designed to account for these delays (or, more generally, utilizing more measurement in the evaluation). Side-channel noise grows when the adversary collects more observations. Side-channel threats that may be identified in hardware design phases can also be detected using security analyzer, which falls under category one. You may test for both the attack vulnerabilities and the efficacy of the structural adjustment needed to avoid timing and cache assaults using commonly available vulnerability assessment software platforms. All existing security assessment platforms should be used at each step of the hardware project cycle to construct a Secure Design Phase for equipment, which is the most complete approach to this protective measure.

When a target's calculation time is quantized into discrete clock cycles, isochronous software acts as an effective countermeasure. As a consequence, timing attacks becomes more difficult. Containment techniques are difficult to devise due to the fact that even individual instructions on certain CPUs may vary in timing. Basic power assaults may be somewhat countered by the "program counter security paradigm"; however, it does not protect against differential power-analysis attacks. It is not necessary to have access to secret values in order to run a PC-safe software. Because the whole public has access to this information, all conditional branches depend on this knowledge. Isochronous code restricts you more than branch-free code, so you will have less options. No matter how powerful a CPU may be, the usage of a constant execution route prevents secret information from being leaked due to power disparities based on how the functions are performed (power variations while choosing a single branch over the other). In systems whose program execution duration is independent of data, PC-secure programs are similarly protected against timing assaults.

This information may be gleaned from modern CPUs' memory cache since accessing data that is seldom utilized has a large delay penalty. The use of memory in a predictable way prevents cryptographic code cache threats (e.g., gaining access to inputs and program information, and completing this based on fixed patterns) For instance, data-dependent file lookups must be banned since the caching could indicate which table area was requested. The Dynamic Differential Logic circuits (DDL) known as SABL are offered as a hardware solution when just one switching event occurs per one cycle. (Sense Amplifier Based Logic). DDL-based hardware has a third choice in the form of Wave Dynamic Differential Logic (WDDL). An alternative to scalable hardware designs was proposed as the Pipeline Current Flattening Module (PCFM) and Flattening Feedback Module (FCFM). Georg, Knöös and McClean [28] claims that one core may receive both the input data and the private keys. Using the modified double-width AES technique, the input keys are copied; private keys reversed; and the output keys are generative from the initial one.

Cybercriminals may be able to bypass common hardware and software security measures using attacks like DPA and SPA. DPA may do in seconds what cryptoanalysis and brute force techniques could not in hours or days. Additionally, the non-intrusive nature of these technologies allows attackers to steal personal information without discovery. As a result, it is necessary to take prophylactic measures; while it is simple to avoid SPA. The system's real workings may be obscured by random activities. There should be no conditional branching and no inconsistent execution paths. Preventing DPA is more difficult than it used to be. Assaults involving DPA have occurred throughout the years. It is possible to begin by lowering one's sensitivity to background noise, which will need a greater number of traces for an assault. Temporal noise may be introduced to a design by using unpredictable wait states, random data, or false processes. This method may be seen in Kilopass' SecretcodeTM memory. During memory reading, random data is injected into the bus in an effort to mask out the output.

It is quite possible to balance the amount of power needed for each data point or computing phase separately. Complimentary logic or steady weight coding may be used to achieve this. The magnitude of the divergent signal would be reduced if power usage was controlled. Kilopass' Secretcode memory is a nice illustration of this. To represent each bit in the memory, a bit-bar has been created. When memory contents are read out, there are always the same number of 1s and 0s. For example, a password timeout may be used to avoid side-channel attacks by restricting the number of transactions that can be made with one key. If a key has been used 1000 times, it is no longer usable and must be changed with a new key. The bulk of present DPA efforts would be eliminated if this were the case.

Using effective and low-cost cryptographic implementation of the encryption methods may help prevent these assaults. A Binary Expansion algorithm with a random starting point is being used to disrupt DPA and RPA/ZPA. In order to avoid MESD and ZESD, it was recommended that a randomized value (r) be used for message masking preparatory to multiplications and that exponent masking be used to prevent SEMD. The inclusion of random multiples of (N)= (p - 1) may hide the exponentiation (q - 1). ê = e+ (N). A right-to-left binary computation method is used to move from the initial random position towards the MSB, then the left-to-right binary multiplications technique is used to move towards the LSB. To counteract the CPA attack, the authors in [29] developed a randomised window-scanning RSA system that is impervious to power usage analysis assaults. Putting the bits back in the right sequence will be tough even if the adversary has recovered the bits.

Similar approaches employed for RSA may be utilized in a different context to attack AES hardware implementations. However, several AES defenses have been targeted by hackers. For instance, the multi-round vulnerability assessment attack aims to breach block cipher technique protections. Several defenses against AES power assessment techniques have been put in place, including random screening and device rebalancing. Hardware balancing approaches, for example, have a reputation for being expensive because of their high cost. The high power and energy consumption levels of hardware approaches owing to sophisticated modular arithmetic operations, such as divisions and multiplication, are the cause of hardware's high cost. To save money, a balancing mechanism called MUTE is presented in [30] that only utilizes the auxiliary processor when necessary. This balancing solution uses MPSoC (Multiprocessor System-on-Chip) to run concurrent AES algorithms. On one of the multiprocessors, the initial AES is run with the original encryption algorithm, while the updated AES is run with the new secret key.

VII. CONCLUSION

In order to calculate, communicate, and regulate environmental or human-made events, CPSs use co-engineered, networked computer technology. High-quality services are provided by the CPSs, which are closely linked. There are a number of distinct systems that make up Cyber-Physical Technologies, including humans, embedded devices, intelligent devices and physical settings. There are several uses for Cyber-Physical Systems in our day-to-day lives as well as in the domains of industry, manufacturing, and the armed forces. Information security, privacy issues, and the need to balance security with performance are just a few of the many obstacles that CPSs must deal with. For CPSs, conventional data security methods are not the best solution, since they are resource-deprived and need huge requirements to provide adequate security. On Cyber-Physical Systems (CPS), we gave a brief outline of their essential properties, the technology that support them as well as security threats. We also spoke about a common side channel attack i.e., the Differential Power Analysis (DPA) and how to protect against it in the context of AES and RSA.

Data Availability

No data were used to support this study.

Conflicts of Interest

The author(s) declare(s) that they have no conflicts of interest

References

[1]. S. Yadav, "A resilient hierarchical distributed model of a cyber physical system", Cyber-Physical Systems, pp. 1-24, 2021. Doi: 10.1080/23335777.2021.1964101.

[2]. I. Gronau and S. Moran, "Optimal implementations of UPGMA and other common clustering algorithms", Information Processing Letters, vol. 104, no. 6, pp. 205-210, 2007. Doi: 10.1016/j.ipl.2007.07.002.

[3]. B. Susmita, D. Parween and V. Nikitha Reddy, "Security Challenges Faced Due to Increasing Data", International Journal of Scientific and Research Publications (IJSRP), vol. 8, no. 12, 2018. Doi: 10.29322/ijsrp.8.12.2018.p8431.

[4]. S. Yadav, "A resilient hierarchical distributed model of a cyber physical system", Cyber-Physical Systems, pp. 1-24, 2021. Doi: 10.1080/23335777.2021.1964101.

[5]. T. Chen, "On kernel design for regularized LTI system identification", Automatica, vol. 90, pp. 109-122, 2018. Doi: 10.1016/j.automatica.2017.12.039.

[6]. A. Oluwafolake and O. Solomon, "A multi-algorithm data mining classification approach for bank fraudulent transactions", African Journal of Mathematics and Computer Science Research, vol. 10, no. 1, pp. 5-13, 2017. Doi: 10.5897/ajmcsr2017.0686.

[7]. J. Xiao, "Trajectory planning of quadrotor using sliding mode control with extended state observer", Measurement and Control, vol. 53, no. 7-8, pp. 1300-1308, 2020. Doi: 10.1177/0020294020927419.

[8]. H. Power, "New solution to a problem in Luenberger observer design", Electronics Letters, vol. 11, no. 3, p. 65, 1975. Doi: 10.1049/el:19750050.

[9]. R. King and M. Phipps, "Shannon, TESPAR and approximation strategies", Computers &amp; Security, vol. 18, no. 5, pp. 445-453, 1999. Doi: 10.1016/s0167-4048(99)80111-4.

[10]. "Call for Contributions Special Issue on Cyber Security for Embedded Controls in Cyber Physical Systems", IEEE Design &amp; Test, vol. 34, no. 6, pp. 127-127, 2017. Doi: 10.1109/mdat.2017.2772155.

[11]. R. Ivanov and I. Raykov, "Parametric lyapunov function method for solving nonlinear systems in hilbert spaces", Numerical Functional Analysis and Optimization, vol. 17, no. 9-10, pp. 893-901, 1996. Doi: 10.1080/01630569608816732.

[12]. L. Sepmeyer, "Prediction of Command Control System Dependability and Performance", IRE Transactions on Reliability and Quality Control, vol. -11, no. 3, pp. 35-42, 1962. Doi: 10.1109/ire-pgrqc.1962.5009617.

[13]. R. Dhaouadi and K. Kubo, "A nonlinear control method for good dynamic performance elastic drives", IEEE Transactions on Industrial Electronics, vol. 46, no. 4, pp. 868-870, 1999. Doi: 10.1109/tie.1999.778264.

[14]. S. Wildhagen, F. Dürr and F. Allgöwer, "Rollout event-triggered control: reconciling event- and time-triggered control", at - Automatisierungstechnik, vol. 70, no. 4, pp. 331-342, 2022. Doi: 10.1515/auto-2021-0111.

[15]. Y. Ma, W. Che and C. Deng, "Dynamic event-triggered model-free adaptive control for nonlinear CPSs under aperiodic DoS attacks", Information Sciences, vol. 589, pp. 790-801, 2022. Doi: 10.1016/j.ins.2022.01.009.

[16]. D. Schaller, M. Hellmuth and P. Stadler, "A simpler linear-time algorithm for the common refinement of rooted phylogenetic trees on a common leaf set", Algorithms for Molecular Biology, vol. 16, no. 1, 2021. Doi: 10.1186/s13015-021-00202-8.

[17]. N. Zhang, X. Gao and T. Yu, "Heuristic Approaches to Attribute Reduction for Generalized Decision Preservation", Applied Sciences, vol. 9, no. 14, p. 2841, 2019. Doi: 10.3390/app9142841.

[18]. F. Uribe, I. Papaioannou, Y. Marzouk and D. Straub, "Cross-Entropy-Based Importance Sampling with Failure-Informed Dimension Reduction for Rare Event Simulation", SIAM/ASA Journal on Uncertainty Quantification, vol. 9, no. 2, pp. 818-847, 2021. Doi: 10.1137/20m1344585.

[19]. M. Hamdan and M. Mahmoud, "Secure Filter for Discrete-Time Delayed Systems Subject to Cyber Attacks", Cyber-Physical Systems, pp. 1-23, 2021. Doi: 10.1080/23335777.2021.1916230.

[20]. C. Li and P. Tam, "An iterative algorithm for minimum cross entropy thresholding", Pattern Recognition Letters, vol. 19, no. 8, pp. 771-776, 1998. Doi: 10.1016/s0167-8655(98)00057-9.

[21]. G. GUO and B. WANG, "Robust Kalman Filtering for Uncertain Discrete-time Systems with Multiple Packet Dropouts", Acta Automatica Sinica, vol. 36, no. 5, pp. 767-772, 2010. Doi: 10.3724/sp.j.1004.2010.00767.

[22]. T. ZHANG and M. FAN, "Countermeasure for Cryptographic Chips to Resist Side-Channel Attacks", Journal of Software, vol. 19, no. 11, pp. 2990-2998, 2009. Doi: 10.3724/sp.j.1001.2008.02990.

[23]. H. LIU, X. ZHAO, T. WANG, S. GUO, F. ZHANG and K. JI, "Research on Hamming Weight-Based Algebraic Side-Channel Attacks on SMS4", Chinese Journal of Computers, vol. 36, no. 6, pp. 1183-1193, 2014. Doi: 10.3724/sp.j.1016.2013.01183.

[24]. "ENSURING PRIVACY ON E- MEDICAL HEALTH CARE USING TRIPLE-DES ALGORITHM", International Journal of Recent Trends in Engineering and Research, vol. 3, no. 3, pp. 201-207, 2017. Doi: 10.23883/ijrter.2017.3068.zfrnx.

[25]. S. Akiyama and Y. Tanigawa, "The Selberg trace formula for modular correspondences", Nagoya Mathematical Journal, vol. 117, pp. 93-123, 1990. Doi: 10.1017/s0027763000001823.

[26]. F. Gosselin, "Test of mathematical assumptions behind the `incidence function' estimation process of metapopulations' dynamic parameters", Mathematical Biosciences, vol. 159, no. 1, pp. 21-32, 1999. Doi: 10.1016/s0025-5564(99)00018-8.

[27]. P. Sahil Gupta, "Speech Enhancement Using Modified Spectral Subtraction Algorithm", International Journal Of Engineering And Computer Science, 2016. Doi: 10.18535/ijecs/v4i12.35.

[28]. D. Georg, T. Knöös and B. McClean, "Current status and future perspective of flattening filter free photon beams", Medical Physics, vol. 38, no. 3, pp. 1280-1293, 2011. Doi: 10.1118/1.3554643.

[29]. M. Joye and Sung-Ming Yen, "Optimal left-to-right binary signed-digit recoding", IEEE Transactions on Computers, vol. 49, no. 7, pp. 740-748, 2000. Doi: 10.1109/12.863044.

[30]. L. SHI and Z. HE, "Adaptive load balancing model based on prediction mechanism", Journal of Computer Applications, vol. 30, no. 7, pp. 1742-1745, 2010. Doi: 10.3724/sp.j.1087.2010.01742.