Multi-Level Fusion for Enhanced Host-based Malware Detection in ICT-Enabled Smart Cities

Alaa Q. Raheema[1], Massila Kamalrudin[2], Nur Rachman Dzakiyullah[*2,3]

[1] Civil Engineering Department, University of Technology, Baghdad, Iraq
[2] Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka, Melaka, Malaysia
[3] Faculty of Computer and Engineering, Department of Information System, Universitas Alma Ata, Yogyakarta, Indonesia
Emails: 40345@uotechnology.edu.iq; massila@utem.edu.my; nurrachmandzakiyullah@almaata.ac.id

Abstract

In smart cities, the widespread adoption of Information and Communication Technologies (ICTs) presents both opportunities and challenges for security. While ICTs enable increased productivity, data sharing, and improved citizen services, they also create new vulnerabilities for malicious actors to exploit. This necessitates robust host-based security solutions to protect critical infrastructure and data. This paper proposes a novel multi-level fusion approach for enhanced host-based malware detection in ICT-enabled smart cities. By leveraging diverse data sources and employing advanced fusion techniques, our approach achieves significant improvements in malware detection accuracy, network evaluation, and security analysis compared to existing methods. Specifically, our proposed approach demonstrates a 72.1% malware detection rate across various attack scenarios, 69.7% accuracy in host network evaluation, 82.8% reduction in security analysis error, 75.4% accuracy in network probability detection, and an overall accuracy of 67.2%. These results showcase the potential of multi-level fusion for strengthening host-based security in smart cities. This approach offers several advantages over traditional host-based security solutions. Firstly, it provides more comprehensive threat detection by utilizing multiple data sources. Secondly, it reduces the burden on IT administrators by automating security analysis and decision-making. Finally, it enables continuous improvement through adaptive learning and feedback mechanisms. Overall, our multi-level fusion approach represents a promising advancement in host-based security for ICT-enabled smart cities. It offers significant improvements in accuracy and efficiency, paving the way for a more secure and resilient urban environment.

Keywords: Smart City; Host Security; Malware Protection; Technological Development; Information and Communication Technology.

1. Introduction

With the explosion in ICT technology, communication services have also improved. This kind of expansion comes with a new set of security issues [1][2]. The smart home is one of the more well-known uses of ICT and also presents a serious security challenge in thwarting attacks from unknown sources. Following that, communities use this information to enhance their infrastructures, community utilities such as electricity, and various other aspects [3]. When it comes to a smart city, it leverages technology to deliver services and handle municipal issues. Things like better public transit, more comprehensive social services, and a focus on environmental responsibility make a city smart [4]. Some examples of how cities use innovative technology to develop inventive solutions to

Doi: https://doi.org/10.54216/FPA.150220
Received: August 08, 2023 Revised: December 16, 2023 Accepted: April 09, 2024

their most severe urban concerns include Columbus, Pittsburgh, Denver, San Francisco, and Dallas [5]. As these five cities indicate, they show no one blueprint for constructing a smart city. A smart city is built by its residents. They play an active role in the city's development and operations [6]. If they live in a typical metropolis, they may not even know that a problem exists.

On the other hand, a smart city empowers residents to spread awareness of issues and give suggestions for remedies [7]. From where to invest to where to have lunch, a smart city can assist its residents with their daily choices. Organizations like restaurants, retail shops, dry cleaners, and so on will be able to locate their new locations based on the city's foot traffic [8]. Smart cities aim to enhance the quality of life for their residents by focusing on such fundamentals as policy efficiency, waste reduction, daily challenges, social and economic quality, and social inclusion [9]. More than merely being more efficient to operate, data-driven cities are more liveable, and living in one is a more pleasurable experience [10]. Decisions made by cities throughout the globe are becoming more data-driven and, hence, better for the residents and the environment. Based on innovative solutions, the ICT-enabled Smart City program aims to enhance the lives of its residents while improving and stimulating economic growth [11]. Smart cities can better manage resources and provide government services faster at reduced operating costs. In reality, the municipality may recoup its costs by reselling the data it collects from connected systems, and it's a cinch to make the decision [12]. Smart cities and businesses rely heavily on cutting-edge ICT to advance public and private environments like buildings, hospitals, and transportation. New computing paradigms have converged on continuously optimizing resource distribution to boost service quality.

Host security represents a group of security measures implemented on the computer's operating system [13]. Tools that monitor traffic on and off the machine on which they are installed are instances of host-based security. Allowing IT executives to concentrate on the most critical patches is one of the advantages of host-based security. The IT paradigm, ICT, and IC are integrated into a unified system for manufacturing improvement, data exchange and security, and scalability. [14]. Direct contact with an infected machine may cause havoc on an organization's infrastructure if no host-based guarantee exists [15]. The server's security is determined by how it is configured to perform the following functions: Prevention of attacks—minimizing damage to the entire system in the event of a successful assault [16]. On the other hand, a host-based shield is a software or suite of applications built on a single computer that protects the host from the internet and other networks [17].

A host-based firewall is a program installed on a user's system or networked device. [18]. Various firewalls can prevent the spread of viruses and malware across networks and safeguard each host from attack. A host-based penetration testing keeps tabs on the computer network it is placed on, scanning for suspicious activity and recording it [19]. A host security system can keep a close eye on essential security systems. The inability to detect typical reconnaissance attempts against the hosting or a range of hosts is a drawback of using an integrated hosted device [20]. Employing network sensors strategically dispersed across the network is the foundation of network-based layers [21]. They monitor and analysed every traffic passing across the local area network. The low-level functioning can be monitored using host-based devices, but the services that execute on that host cannot [22]. One can only use host-based monitors on peers that they were aware of. They need to locate unauthorized hosts before they can keep track of them. Protection from untrusted networks: mobile systems may be protected from untrusted networks using a host-based firewall [23]. The same program's vulnerable competitors may be protected by it.

Many technology firms use the smart city to describe integrating infrastructure and social services such as structures, transit, electricity, and pumping stations into a single, easier, and more efficient system [24]. Large and small districts are already proposing a new city concept, described as the smart city, that symbolizes a medium-sized, networked, and ecological neighbourhood that is pleasant, beautiful, and secure [25]. Local needs and environmental constraints are significant in the decision [26]. The system functionality pertains to a computer structure that allows for a management program of all its components utilizing various technology tools that help assemble and analysed data to achieve efficiency, sustainability, productivity, and safety goals [27]. The smart city idea emphasizes the role of technology in boosting a city's profile. Value-added services for city administration and citizens are central to the smart city concept, which aims to employ cutting-edge technology to achieve that goal. Urban Internet technologies are meant to serve that goal.

Doi: https://doi.org/10.54216/FPA.150220
Received: August 08, 2023 Revised: December 16, 2023 Accepted: April 09, 2024

The report explains why cybersecurity is crucial for smart cities, citing the increasing danger of cyberattacks and the need to safeguard vital infrastructure. It emphasizes the necessity for the security of networked devices and the importance of new technologies like the Internet of Things (IoT) in creating smart cities. This paper offers concrete recommendations for improving smart city cybersecurity, such as installing antivirus and anti-malware programs and installing intrusion detection systems. Consistent with industry standards, it stresses the significance of preventative cybersecurity measures, including routine malware scanning and intrusion detection. In addition, the article addresses the topic of risk management in smart cities, outlining an approach that may be taken to lessen the harmful effects of digital urbanization. Given the dynamic nature of cyber threats and the rapid development of smart city technologies, this study is particularly timely and relevant to the continuing conversations about protecting cities in the digital era.

The main contributions of this research are:

- The article uses ICT-enabled Smart City-based Host security (ICT-SC-HS) to safeguard the smart city from cyberattacks. A single infected machine might destroy the enterprise's systems without host-based protection.
- Host-based barriers include network security applications on computers and devices. These firewalls prevent dangerous network infestations. Hosts can avoid viruses and malware. Each server's host-based firewall controls access and traffic.
- Thus, compared to previous research, the proposed article shows malware detection in different attacks at 72.1%, host network evaluation at 69.7%, absolute errors of security analysis at 82.8%, network probability at 75.4%, and accuracy at 67.2%.

The remaining sections of the paper are structured as follows. Section 2 presented several scholarly articles that address this topic. Section 3 discusses the methodology for the use of SC-HS to provide host security in a smart city. The research analysis is discussed in greater detail in Section 4. Section 5 discusses the study's findings and their implications for the future.

2. Related Work

Yuanzhang Li et al. (2021) [28] accessed that protecting data and enhancing system security may be accomplished via security monitoring and analysis. As far as security management analysis is concerned, there are several viable options. The Dempster–Shafer (DS) evidence theory is used in this research to offer a host security analysis approach. Gradient boosting, multiple linear, and K-nearest neighbour regression are three of the models used as sensors for the integration of several sources of data. The findings of the various sensors' security analyses are used as evidence to support the DS evidence hypothesis. The server is sufficiently protected from threats utilizing this method, as measured by the following error metrics: mean relative percentage error, root-mean-square error, and absolute numbers error. The diversity of available data sources may impact the proposed method's effectiveness when used for security analysis, which may introduce noise or biases.

Frederick Hauser et al. (2020) [29] proposed media access protocol security (MACsec), a widely used IEEE standard for protecting Layer 2 infrastructures, to safeguard P4-MACsec networks among P4-based SDN devices. Many switches and routers support access control protocol security. Unlike VPN protocols like IPsec, it has very few performance limits on these devices. To administer a global link map safely and efficiently, we suggest an innovative technique that uses protected LLDP frames and a two-tier control plane structure. If there is an observed relationship between P4 targets, the P4 targets may be automatically configured to use MACsec to construct secure channels between them, produce keying material, and perform other tasks. It can detect connection modifications and perform rekeying to ensure that MACsec runs securely without any setup. Although P4-MACsec has fewer limits than other security solutions, this research explores potential constraints based on network conditions, volume of traffic, and hardware processing capabilities.

Eder Ollora Zaballa et al. (2020) [30] explained the data plane functions may now be delegated to Software-Defined Networks (SDNs) and programmable data planes, resulting in the ability to free up resources for other applications and services. Using the P4 programming language, data planes

Doi: https://doi.org/10.54216/FPA.150220
Received: August 08, 2023 Revised: December 16, 2023 Accepted: April 09, 2024

may be tailored to suit the application's needs. For example, it may enhance network security by providing packet processing capabilities. The firewall functionalities effortlessly allow deployment in the data plane, and port knocking aims to prevent hosts from dealing with unwanted traffic. To install the port knocking service in this manner, P4Knocking may be more transparent and efficient than a host-based approach. Network security tool P4Knocking, however, needs to be extensively examined for vulnerabilities to prevent security breaches and illegal access.

Robin Gassais et al. (2020) [31] described interconnectivity and creativity in the environment as being unleashed thanks to the rise of the Internet of Things (IoT). Working remotely with many previously distinct devices has dramatically improved efficiency and organization. However, due to this, the number of security flaws is increasing. Therefore, there is a growing risk to the privacy and safety of smart device users from attacks that make advantage of or specifically target these devices. Additionally, the wide range of technologies involved in the IoT makes it challenging to design security measures for smart devices [41]. When an intrusion occurs, our system uses tracing methods to get device activity automatically, processes this data into numeric arrays to train numerous machine learning algorithms, and raises warnings. The study emphasizes the need for accurate intrusion detection systems, calling attention to the need to know the rates of false positives and false negatives and taking steps to reduce them.

Jingping Liu et al. (2020) [32] admitted industrial Cyber-physical systems (ICPSs) are massive, distributed, inconsistent, federated, and life-critical. Hence, this paper examines a breach recognition scheme that protects from all-around safety threats based on the architecture and the kinds of attacks of each layer. Cyberspace uses anomaly monitoring of the statistical distribution of network transmission characteristics of the data transmission layer, which incorporates a forgetting factor-induced recursive Gaussian mixture model (FF-RGMM), to detect cyberattacks. An application control layer regularised sparse deep belief network model detects abusive behavior to prevent assaults. The research stresses the need for updates, patches, and compliance with developing ICPS technologies, highlighting the significance of these measures for the long-term upkeep and viability of intrusion detection systems.

Samuel Oyewole et al. (2020) [33] discussed military facilities have mushroomed in response to the government's expanding military capabilities, responsibilities, and interest in conducting internal security operations around the country. Locals have mixed feelings about the army's presence and scheduled events in and near military installations because of their positive and negative effects on the host community's growth and safety. There has been a lack of governmental and scholarly attention to these critical developments for military readiness and its democratic consolidation, peace, security, and worldwide image.

Panjun Sun et al. (2020) [34] proposed to examine the current state of cloud computing security research from the standpoint of different cloud-based privacy security systems. First, we'll go through some of the privacy and security problems associated with cloud computing and provide a strategy for combating them. The paper shows and discusses the progress of several technologies, including access control, stream cipher strategy innate quality cryptographic, key policy attribute-based encryption, the perfect, cross, expulsion process, the detectable framework, proxy re-encryption, hierarchies' authentication, advanced search encoding, and multi-tenant trust, and then compares and analyses the features of each technology. While the study's limitations should not be overstated, they highlight the necessity to compromise privacy protection and system performance.

M Tanjidur Rahman et al. (2020) [35] prepared a non-volatile memory that is believed to hold the key after manufacture by the IP owner. SAT assaults, logic locking, and responses to these attacks have been the primary focus of the research community over the last several years. The whole plot has been compromised. We begin by looking at the potential threats to the locked circuits and their abilities. To prove that even if the vital storage is secure and read-proof, the critical transfer between the key storage and key gates via registers and buffers makes it possible for an attacker to get a copy of a secret. The study needs to consider real-world circumstances in which the adversary faces additional obstacles or limits that could compromise the key extraction process.

Hazem Munawer Al-Otum et al. (2020) [36] accessed color image watermarking for copyright protection is shown in this work. The proposed technique establishes a connection between the sub-bands of the major color components in the wavelet-packet domain. The system's resilience against attacks is enhanced by employing a dual-layer security strategy. Experimental studies and a

Doi: https://doi.org/10.54216/FPA.150220
Received: August 08, 2023 Revised: December 16, 2023 Accepted: April 09, 2024

comparison study demonstrated the superior performance of the proposed method. Despite increased aggression, the results reveal that watermarking is still virtually undetectable. The importance of testing your watermarking scheme's resistance to different kinds of attacks is emphasized throughout the text.

Anuj Dubey et al. (2020) [37] described cipher implementation as the primary focus of research on power-side channels in which machine-learning models are considered intellectual property and hence need strict secrecy to be used. This study adds neural network classifiers to the DPA framework. A neural network's hidden parameters, such as weights and biases, may be extracted through DPA attacks during inference. It suggests first-line defenses against these assaults, including strengthening masked communication. The final design uses masked adder trees, masked rectifier linear units, and other unique masked components for fully-connected layers. The effort should assess the degree to which the proposed countermeasures generalize to other models or contexts across different neural network designs and applications.

Steffen Haas et al. (2020) [38] proposed it is possible to detect assaults and intrusions by analyzing network traffic using intrusion detection systems (IDS). Aside from a lack of visibility because of encrypted communication, clever attackers aim to avoid detection. To circumvent these constraints, we add extra data from the hosts to the scope of Network IDSs (NIDS). The assigned network flows to processes and user platforms that can gather, evaluate, and correlate data from hosts and networks on a massive scale. Detection scripts may be easily added to the forum, employing the previously correlated but newly obtained and constantly updated host data. With a distributed deployment, they may use as many query hosts as possible. The language stresses the importance of preventing unauthorized access and breaches to host data gathered, processed, and kept by your platform.

Jae-Myeong Lee et al. (2020) [39] accessed an increase in the sophistication of cyber assaults against Supervisory Control and Data Acquisition systems (SCADA)—the malware assaults on the SCADA host system software vulnerabilities and control host processes. According to the findings of this study, a malicious program uses Dynamic Link Library (DLL) Injection to infiltrate SCADA host processes. We have proposed a security mechanism, a DLL Injection blocking method, which we've implemented as a library and tested against various DLL Injection situations to demonstrate its efficiency in protecting against real-world malware that uses this approach. The effort must ensure the proposed solution is compatible with multiple SCADA environments, including architectures, vendor-specific configurations, and legacy systems.

Table 1: Survey On the Existing Methodologies

Author Name	Methodology and Approach	Findings	Research Gap/Limitations
Yuanzhang Li et al. (2021) [28]	DS evidence theory for host security analysis; numerous models as sensors; error metrics evaluation.	Error metrics assessment and reinforced server security.	Lack of discussion of effectiveness, the possibility for noise, or biases in security assessments when using many data sources.
Frederick Hauser et al. (2020) [29]	MACsec, a novel approach to link map security, is being implemented in P4-based SDN devices.	Exploring potential limits depending on network characteristics for achieving effective and secure P4-MACsec networks.	Inadequate discussion on performance under many network environments.
Eder Ollora Zaballa et al. (2020) [30]	P4Knocking is used for port knocking and other firewall-related data plane activities.	Improved network safety with P4Knocking's openness and effectiveness.	Comprehensive testing of P4Knocking's weak spots is required.
Robin Gassais et al. (2020) [31]	Detecting intrusions in the Internet of Things by means of machine learning by tracking	Reliable intrusion detection for Internet of Things gadgets, emphasizing reducing false positives.	The difficulty of developing adequate safety protocols for the wide range of IoT

Doi: https://doi.org/10.54216/FPA.150220
Received: August 08, 2023 Revised: December 16, 2023 Accepted: April 09, 2024

	device behavior.		technology is rarely discussed.
Jingping Liu et al. (2020) [32]	Anomaly detection scheme, FF-RGMM, for industrial Cyber-physical systems that can detect security breaches.	System updates and compliance measures are emphasized, focusing on cyberattack detection in ICPSs.	Updates, fixes, and compliance details are not specified.
Samuel Oyewole et al. (2020) [33]	Effects, expansion, and local security at military installations are discussed.	Host communities have a range of reactions to military presence and activities, yet the topic has received little academic attention.	Limited focus on technical facets of security.
Panjun Sun et al. (2020) [34]	Analysis and comparison of several cloud security solutions.	Various privacy security systems are discussed, and their features are compared and contrasted.	Study limitations mentioned but not detailed.
M Tanjidur Rahman et al. (2020) [35]	Research into the safety of non-volatile memory, including assessing potential dangers.	Recognizing potential attacks on secured networks and planning for recovering access keys.	Real-world examples and other unsuspected challenges need to be investigated.
Hazem Munawer Al-Otum et al. (2020) [36]	Dual-layer security, including color image watermarking for copyright safeguards.	Strengthened resistance against attacks; watermarking is nearly unnoticeable.	Testing for resilience to various attacks is emphasized but not further upon.
Anuj Dubey et al. (2020) [37]	The protection of intellectual property through the incorporation of neural network classifiers into a DPA framework.	Masked components for fully connected layers protect from DPA assaults.	The extent to which countermeasures can be used in other settings is ignored.
Steffen Haas et al. (2020) [38]	Distributed implementation of NIDS using host data for traffic analysis over the network.	Distributed deployment for scalability, and enhanced host-based intrusion detection.	No specifics were provided regarding host data security or access management.
Jae-Myeong Lee et al. (2020) [39]	Method for preventing DLL injection in SCADA systems; scenario testing.	Effectiveness in defending SCADA systems from DLL Injection; compatibility with actual malware.	Compatibility with existing SCADA and other systems is glossed over.

As tabulated in Table. 1, a complete literature survey is conducted on the host security protection for malware attacks and their various applications. The most considerable research is summarized here. Numerous researchers and studies in cybersecurity use multiple approaches, data sets, and evaluation criteria. Cyber threats constantly change and adapt; their manifestations might vary widely depending on the circumstances. As a result, it could be difficult to make an objective comparison. In the paper, the researchers implemented the SC-HS technique to explore smart cities' features with host security protection from cyber-attacks and its experimental analysis.

3. Proposed Theory of Host Security Protection in The Smart City

There are several ways to secure systems and networks against cyber-attacks, including various technologies, procedures, and policies. Anti-cyber assaults and technology exploitation are the primary goals of this program. Antivirus software should scan any files that they download before they open them. They may check the whole machine for malicious code using antivirus software. To discover malware early and prevent it from spreading, they should conduct frequent scans on the computer. The second line of defence against malicious software is provided by anti-malware software. Antivirus software is critical to any computer system's technical reasons, whether for

Doi: https://doi.org/10.54216/FPA.150220
Received: August 08, 2023 Revised: December 16, 2023 Accepted: April 09, 2024

home use or in a professional setting. Threats in the digital world are constantly changing. An anti-malware program can identify new viruses, while an antivirus program can guard against the most prevalent ones. Malware of the second generation, which traditional antivirus software often fails to detect, is protected by anti-malware software [47]. Antivirus software protects your computer from malicious software that could compromise the data, slow down or even shut down the machine, or allow spammers to use your email account to send unwanted messages. Malicious attachments and emails are filtered out by antivirus software. Antivirus software can protect the computer against many threats, including trojans and viruses. So, installing an antivirus and an anti-spyware program isn't necessary; only the antivirus program will do the job.

The following Figure 1 gives the general structure of a smart city. Figure 1 emphasizes addressing traffic management, parking accessibility, and wait times to enhance urban environments. Efficiencies and sustainability in urban environments are the goals of "smart city" initiatives that employ cutting-edge technologies, data-driven insights, and networking. They encourage eco-friendly modes of transportation, public engagement, efficient traffic management, informed policymaking, a low environmental impact, and long-term stability. Green policies, conservation of resources, and environmentally responsible city development are prioritized in these settlements. Cities can improve their resilience and adaptation to new urban challenges by using innovative and sustainable strategies. The overarching goal of Smart Cities is to improve the lives of city dwellers and lessen their negative influence on the environment.

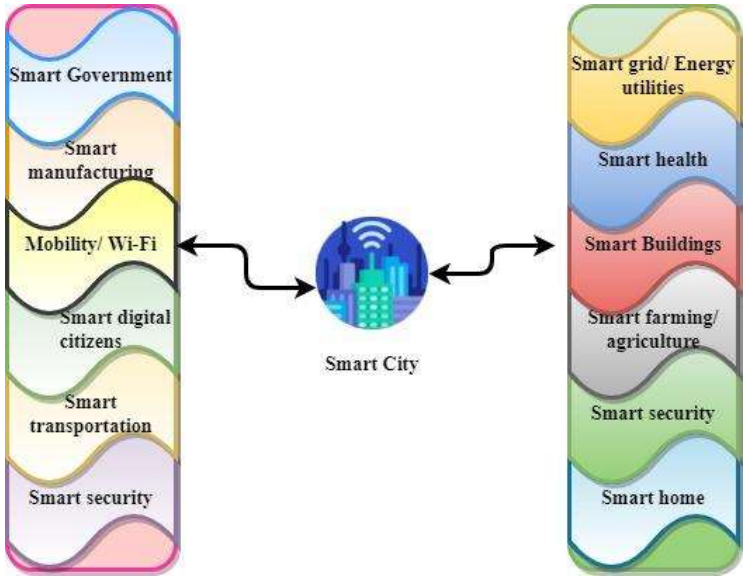

Figure 1: General structure of a smart city

Figure 1 shows that urban management, traffic flow, parking periods, and waits at municipal offices and health facilities should be improved. Improved urban planning and environmental sustainability may be achieved via Smart Cities [44]. They use networking to connect and share information with other individuals, organizations, and institutions to build long-term, valuable partnerships or transfer data across computers. That implies having access to a variety of transportation alternatives that are both safe and ecologically sustainable. Cities and conurbations are conducive to participation in society, and Mobility is a critical factor in this process. Signaling sequences may be improved to increase traffic flow. Moreover, in Figure 2 illustrates the overall structure of the proposed model. IoT data is gathered from many computer systems by the ICT-SC-HS. The system monitors network activity and compares observed data to known attack patterns. The proposed method detects any out-of-the-ordinary actions and verifies whether they resulted from a malicious cyber-attack.

Doi: https://doi.org/10.54216/FPA.150220
Received: August 08, 2023 Revised: December 16, 2023 Accepted: April 09, 2024

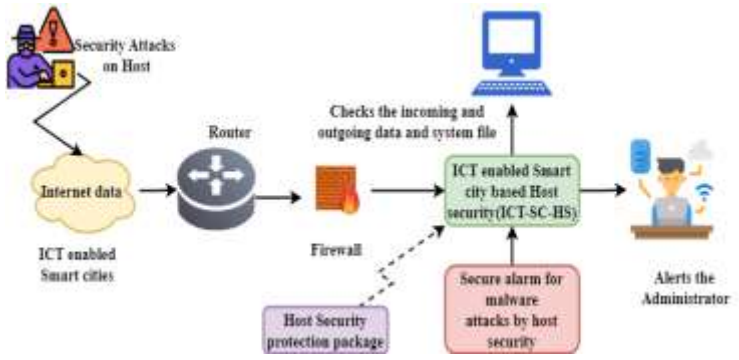

Figure 2: Overall structure of ICT-SC-HS

The safety device will alarm after any suspicious activity has been verified. With these alerts, you can pinpoint the problem's source and end the attack faster. Smart City technology helps communities conserve resources by decreasing power, water, and gas expenses. Automated data storage for energy usage and intelligent systems control is possible with these tools. It is possible to publish a route for traffic inside or across networks called routing. The Public Switched Telephone Network (PSTN) and computer networks like the Internet use routing. Anyone not permitted to access the encrypted information cannot decipher the information [42]. There are various methods by which people or devices may be allowed access to encrypted data, but passwords and decryption keys are the most often used [46]. The mathematical representation of the approach used in this article to improve host security protection in smart cities is shown in Figure 3. When compared to conventional methods, the results shown here are encouraging. A measure of host safety could be the cumulative number of reported cyberattacks and advanced threats. Developing a timeline of threats and responses can help businesses evaluate the efficacy of their security measures after implementation. In the past, Balanced Scorecards have been utilized to elaborate on the interconnections between those four perspectives. The strategic objectives of the data security organization and the value it brings to the firm are reflected in the value it provides.

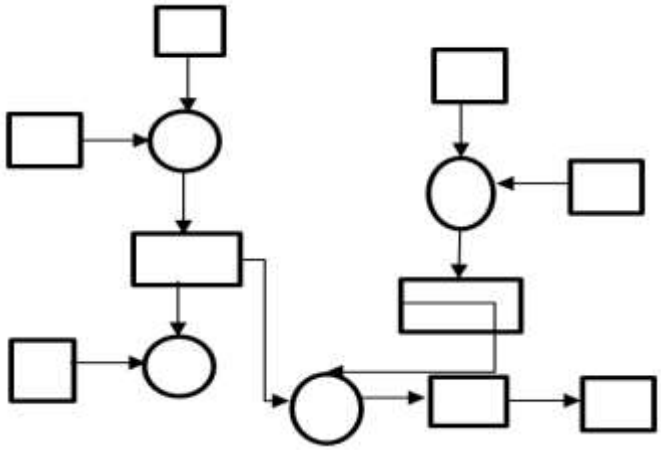

Figure 3: Mathematical illustration of host security protection method

The term information leakage is the illegal disclosure of sensitive information. Data leakage, also known as low and slow data theft, can affect any company, regardless of size or industry.

$$D = c^{-1}\left(\int (f_{\propto}) + c_2\right) \times (g^2) < f_g^{-1} \quad (1)$$

Equation 1 denotes D for smart government, c for smart manufacturing, f for mobility/wi-fi, g for smart digital citizens, $\propto$ and mathematical function for a smart city. Smart Mobility is a defining characteristic of a smart city. It is a revolutionary approach to commuting that promises citizens affordable, multiple modes of transportation, including rapid mass transit systems, on-demand mobility solutions, ride-sharing, vehicle-sharing, electric vehicles, biking, walking, and more.

Doi: https://doi.org/10.54216/FPA.150220
Received: August 08, 2023 Revised: December 16, 2023 Accepted: April 09, 2024

As part of data security access controls, who can access and utilize corporate information and resources, a company's access control policies verify that users are who they claim to be and are authorized to access the data they request via authentication and authorization. Unauthorized acts on the digital assets in an organization's network are explained as network assaults. To change, delete, or steal private data, malicious actors often use network assaults. It is common for attackers to target networks' perimeters to access their own systems' interiors. It is possible to derive meaning from data by studying extensive records. Data-driven, it's a potent tool for diagnosing vulnerabilities, predicting malicious activity, and prescribing countermeasures to guard against it. A heterogeneous network is a network of computers and other devices where the operating systems and protocols vary significantly. Different access technologies may be used to characterize a heterogeneous network. Because of this, cloud computing's main selling point is scalability. Securing an organization's mission-critical infrastructure should be at the core of anticipating growing loads and capacity demands.

$$S = \int v \pm \sqrt{n} * (\gamma^2 < t^2) / \left(\frac{n}{t}\right) - v^{-1} \quad (2)$$

In Equation 2, S for smart security, v for smart transportation, n for smart grid energy, γ for mathematical function, t for smart utilities. Limiting who has access to data and computer systems is the goal of access controls. A data breach might occur if they aren't deployed correctly; however, this is mitigated if used correctly. With built-in computational resources and specified operations to detect certain information, a smart sensor collects input from the physical world and processes the data before sending it. Small, low-power mobile microprocessors are often used to give computing power on the go. It's possible to create a sensor capable of reading, manipulating, and responding to data by embedding it directly into the computer chip! This knowledge is essential for developing more reliable sensors that operate in various temperature, ambient, and pressure settings. Having a healthy and robust constitution is the attribute of being strong and Transposed into the context of a system—the capacity to tolerate perturbations that may damage the system's functional body. Resistance and avoidance are two aspects of resilience, according to specific theories. The idea is that it should only be utilized when essential. Because they use so little power, these gadgets are very convenient. Some models of motion sensors, for example, operate as much as a kilowatt-hour (kWh) of electricity. Smart sensors can store information. Data can be stored on smart sensors since they have a memory unit. Inside the transducer housing, signal conditioning for smart sensors occurs.

$$F = \frac{1}{c} \in \sqrt{k} - j^2 + [w_{-1}] * \int k \left[\frac{j}{2}\right] \% \, w_j \quad (3)$$

Equation 3 refers to F for smart health, c for smart buildings, k for smart farming, j for smart home, w for malware attacks, j for some networks. Malware research is analyzing malware and learning about its components and behavior. For this work, malware will be analyzed using static and dynamic methodologies. Analyzing malicious code using a non-running approach is known as static analysis. The growth of host security assaults is seen in the following figure 4.

Doi: https://doi.org/10.54216/FPA.150220
Received: August 08, 2023 Revised: December 16, 2023 Accepted: April 09, 2024

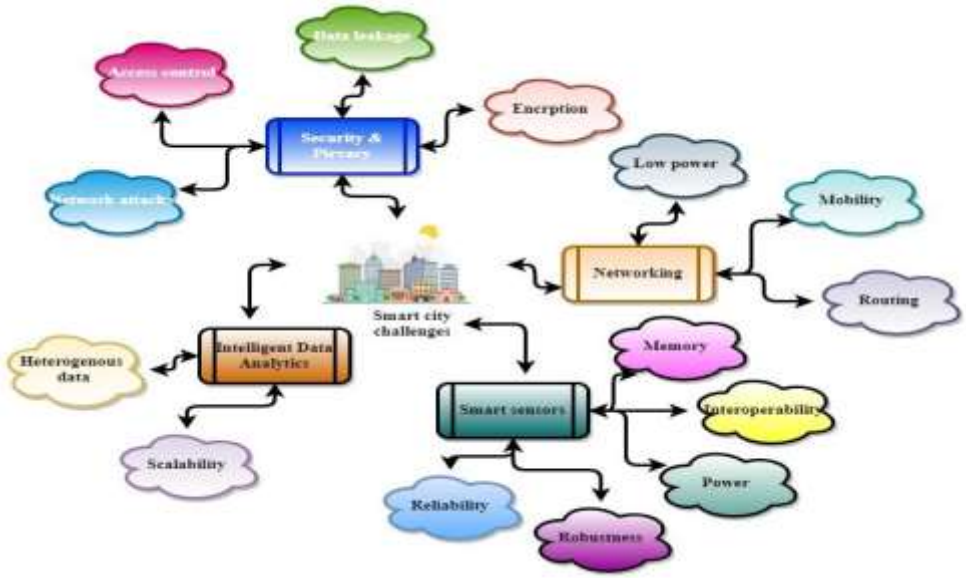

Figure 4: Smart city challenges

Figure 4 expands the urban parking management improvement to improve traffic and parking times, minimize lines and waiting times at municipal offices, and so on. Improved urban planning and environmental sustainability may be achieved via smart cities and added and enhanced green spaces, ancillary areas, and other aspects of the property. The networking process of connecting and sharing data with other individuals, organizations, and institutions fosters collaborative efforts or facilitates data transfer between computers. This context implies having access to safe, quick, environmentally friendly, and cost-effective modes of transportation for education, work, and pleasure. Regarding cities and conurbations, the capacity to engage in society can only be achieved via travel. Signaling sequences may be optimized to enhance traffic flow on the road. By decreasing the power, water, and gas prices, Smart City technology may help communities save money. Automated data storage for energy usage and intelligent systems control is possible with these devices. Routing is establishing a route for data to go inside or across networks. As a general rule, routing may be applied to a wide range of connections, encompassing networks electromechanically like the PSTN and the internet. Encryption aims to make data unreadable to anybody who cannot see it. People or devices may be provided access to encrypted data in various methods, although passwords or decryption keys are the most common. Regardless of size or sector, any firm may suffer from data leakage, often called low and sluggish data theft.

$$V = b_n \left| \sum h"n^{-1} \right| * b_2 \div (j_n^2/s^2) \quad (4)$$

Equation 4 gives V for challenges in smart city, b for networking model, n for low power, h for smart memory, j for interoperability, s for smart sensors. Smart Mobility getting around provides residents with various low-cost transportation choices, including but not limited to rapid mass transit, on-demand mobility solutions, ride-sharing services, vehicle-sharing services, electric vehicles, and more. When protecting confidential information, restricting access is crucial since it determines who can access and utilize sensitive company data and assets. Authorization and authentication are used in access control rules to ensure that only authorized users can access sensitive company information. Attacks on a company's network are a form of cybercrime that targets its digital resources. Offenders frequently employ network attacks to corrupt, destroy, or steal sensitive data. The boundaries of the network are a common target for hackers seeking entry to internal systems. Analyzing datasets to make inferences about their data is known as data analytics. Data-driven, it's a potent tool for diagnosing cybersecurity flaws, predicting future harmful activity, and prescribing countermeasures. It is a term used to describe a computer network when the operating systems and protocols are significantly different. In addition, a heterogeneous network refers to wireless networks with various access methods. Cloud computing's key selling point is its scalability. Scalable security should be the foundation of an organization's mission-critical infrastructure to anticipate growing loads and capacity requirements.

Doi: https://doi.org/10.54216/FPA.150220
Received: August 08, 2023 Revised: December 16, 2023 Accepted: April 09, 2024

$$P = (i + l)\ sin\ sin\ l\ \left\{\frac{1}{i} * m^2\right\} < \iint x_i - i^m \quad (5)$$

Equation 5 reflects P for security and privacy, i for encryption, l for data leakage, m access control, x and data analytics. In a data breach, they help reduce the possibility of information being accessed without proper authorization. With built-in computational resources and specified operations to detect certain information, a smart sensor accepts input from the physical world and processes the data before passing it on. Low-power mobile microprocessors are often used to supply computing resources. However, incorporating the sensor inside the computer chip creates a smart sensor that gathers, processes, and acts on data. The cornerstone for enhanced sensor dependability, even across a wide range of temperature, ambient, and pressure circumstances, is understanding how sensors respond and operate together. A solid and healthy constitution is the quality of being robust. When applied to a system, it refers to its capacity to tolerate disturbances that might alter its functional body. Resistance and avoidance are two aspects of robustness that have been studied. The goal is only to utilize it when required. One of the best things about these gadgets is how little power they use. Several factors affect how much electricity a light bulb consumes, such as how much energy a motion sensor needs. Smart sensors can store data. A memory unit is included in smart sensors, indicating that they can store data. The transducer housing is used to condition the signal from smart sensors.

$$K = \iint f * \left(\frac{m}{-1}\right) \sim g_2 + s^{-1} \neq f^2 \quad (6)$$

Equation 6 denotes K for evaluation of host networks, f for heterogeneous data, m for scalability, g for reliability, s for robustness. Keeping data on a dependable and easily accessible web server is known as data hosting. A long-term commitment is needed to provide a consistent and highly reliable web-connected platform, even if no standard structure exists for delivering this service. The spread of host security attacks is seen in the following figure 5.

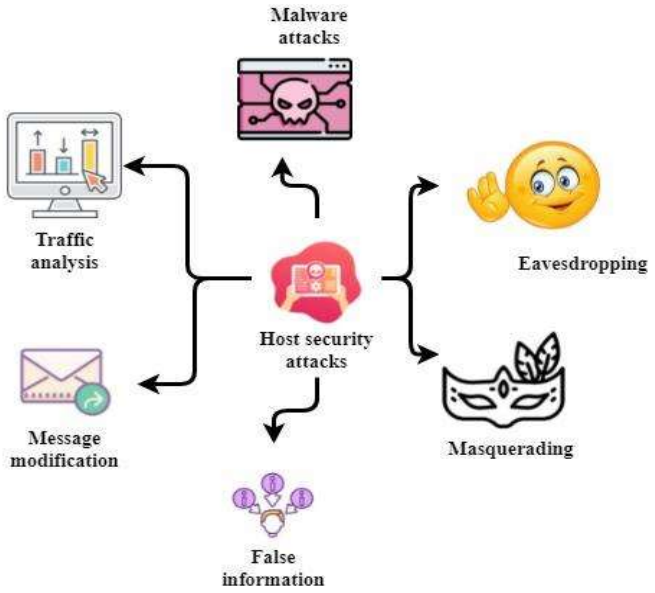

Figure 5: Host security attacks

Figure 5 demonstrates by using a Host header attack, known as Host header injection, an attacker presents a bogus Host header to a web application. This kind of cyberattack uses malware (usually malicious software) to carry out unwanted operations on the system of a victimized party. These assaults fall under malicious software (sometimes known as a virus), including ransomware and spyware. Malware is any program, file, or script harmful to an apparatus or networked site. Understanding the many types of malwares that might infect the computer is essential. Computers,

Doi: https://doi.org/10.54216/FPA.150220
Received: August 08, 2023 Revised: December 16, 2023 Accepted: April 09, 2024

smartphones, and other connected devices may be used to steal data as it is being sent across a network using an eavesdropping attack (called a sniffing or spying attack). The attacker takes advantage of unprotected network traffic to access data being delivered or received by its target. When internet devices are captured by a person for whom they were not intended, eavesdropping is used as an electronic assault. The two primary methods are direct listening to digital or analog voice activation or acquisition or sniffing of data about any communication.\

$$L = log\ log\ x\ "\sqrt[2]{t_x} \leftarrow r_2 * \beta_r + x^{-1} \pm t^r \tag{7}$$

Equation 7 refers to L for host security attacks, x for security information, t for malware attacks, r for unknown access, β for the mathematical function of host security. Attacks on the HTTP Host header take advantage of websites that are prone to attack because of how they handle the value of the Host header. An attacker may insert malicious payloads and control server-side behavior if the server does not verify or escape the Host header. Using a false identity, an attacker may get access to a victim's computer and the information it contains without their knowledge. Masqueraders and traitors are two distinct types of insider attackers who exploit their lawful credentials to achieve illegal ends. As an example of a masquerade assault, financial transaction systems are vulnerable to identity theft. False data injection attacks (FDIAs) were first developed in the smart grid arena. Sophisticated attacks on sensors may create undiscovered mistakes in computations of state variables and values, which the word implies in this context.

$$R = \sum y - \|\sigma_2\| \left[e_y + \frac{1}{-e}\right] * [l_e^2] < y_{-1^l} \tag{8}$$

Equation 8 reflects R for security firewall, y for eavesdropping, e for masquerading, σ for mathematical function, l for lack of security. State or non-state entities may conduct disinformation campaigns to influence people's opinions at home and abroad. As a result of its nature, proponents have urged for misinformation campaigns to be officially categorized as a cyber-threat. The intruder tampering with packet header addresses might redirect a message to a new destination or corrupt the contents on a target system. In most cases, email-based assaults alter notices, and malicious material may be added to an attacker's message body or header fields. A traffic analysis attack uses what the attacker hears on the network, like an eavesdropping attack. By listening to network traffic, the attacker may get information about the location of virtual nodes, the routing topology, and even application behavior patterns. A procedure known as network traffic analysis is used to detect and respond to security risks. Gartner coined it to describe a new product category in the security industry.

$$I = \sqrt[3]{p} \mp w_n^2 \leq \prod \prod (n^2 - p^2) * z_n \approx (p_n) \tag{9}$$

Equation 9 refers to I for absolute errors in security information, p for false information, w for message modification, n for traffic analysis, z for attack detection. To rectify the situation, they may put the server into standby mode and remove it from the server Machine. A difficulty with the authentication process may be to blame if they have a new host. Malware attack alerts are shown in the following figure 6.

Doi: https://doi.org/10.54216/FPA.150220
Received: August 08, 2023 Revised: December 16, 2023 Accepted: April 09, 2024

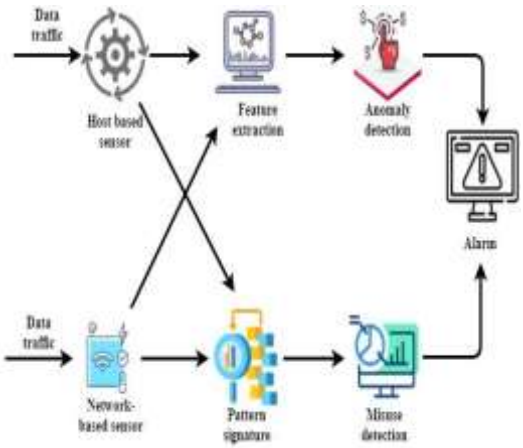

Figure 6: Secure alarm for malware attacks by host security

Figure 6 shows that at any one moment, the volume of data traveling over a network is known as network traffic or data traffic. In computer networks, network data is mainly contained in network packets responsible for the network's burden. As far as can tell, host-based sensors don't offer much information about the services operating on a host. They can only use host-based sensors on hosts they can access and control. They must first locate any unregistered hosts to do any monitoring on them. The information preserved in the original data set; feature extraction involves converting raw data into numerical features that may be processed. It's more effective than using machine learning on raw data. An important component of a signal is its mean window size. It's possible to reduce the amount of data that must be described using feature extraction. The issues resolved still accurately characterize the data, and label feature extraction describes various techniques for building variable combinations.

$$O = \frac{1}{2} * \langle \frac{l_2}{j^2} \rangle + m_l \cong (j_2 * m^{-1}) \emptyset \, \pi/2 \tag{10}$$

Equation 10 denotes O for data traffic, l for a host-based sensor device, j for feature extraction of host security, m for anomaly detection, π for mathematical function, $\emptyset$ for mathematical function. The lack of available bandwidth is perhaps the most frequent source of network congestion. In computing, bandwidth refers to the maximum rate at which data may move through a route – that path's overall capacity, in this context. With too much traffic and insufficient bandwidth to manage it, you're experiencing network congestion. Outlier analysis, known as anomaly detection, is a data mining technique that looks for data points, occurrences, or observations out of the ordinary for the dataset. The presence of anomalous data might signify catastrophic situations, such as a software bug, and opportunities, such as a shift in customer habits. Network assaults may be detected via the misuse detection procedure, which compares current activities to what an intruder would do. Expert systems based on predefined rules are the most common method for detecting abuse nowadays. Attack signatures must be stored in the misuse or signature detection systems database before use. In contrast, an anomaly detection system creates a comprehensive picture of how networks and hosts normally behave. The system is meant to detect intrusions, such as unwanted entrance into a building or other locations, such as a house or school, such as an alarm system called a security alarm. Alarm systems defend against burglary or give fire and intrusion protection in one package.

$$M = tan\ tan\ o\ \pm \beta_i\ \Delta(o^2/i_{-1})\ \forall\ i^2 \tag{11}$$

Equation 11 denotes M for security alarm, o for misuse detection, i for a sensor device, β for mathematical function. It's the process of looking for anomalies that are out of the ordinary and don't fit in with established norms. Outliers, noise, novelty, and exceptions are examples of data anomalies. A signature is a characteristic print or pattern left behind by a malicious assault on a computer network or system in computer security jargon. In network communication, this pattern may be represented as a sequence of bytes in a file. Signature verification is often used in banks and

Doi: https://doi.org/10.54216/FPA.150220
Received: August 08, 2023 Revised: December 16, 2023 Accepted: April 09, 2024

other branch locations to verify signatures. Signature verification software compares an image of a signed document to a database of previously confirmed papers. Sensor networks are electronic devices that collect and send environmental data to a base station. It has been determined that most current security measures and procedures are incompatible with the sensor's design restrictions. A sensor generates electrical signals when it observes a shift in its physical environment. A microcontroller circuit processes the signals. The transceiver takes instructions from the main computer and sends information to another device.

$$T = k^2(q + r) - (k_2) * \sum |q^2 \mp r| \tag{12}$$

Equation 12 reflects T for network-based sensor, k for pattern signature, q for the probability of security, r for security detector. Network analysis procedures are a collection of specific analytical methods utilized when a network of interconnected and related components must be analyzed and optimized—enhancement of host security protection package as shown in figure 7.

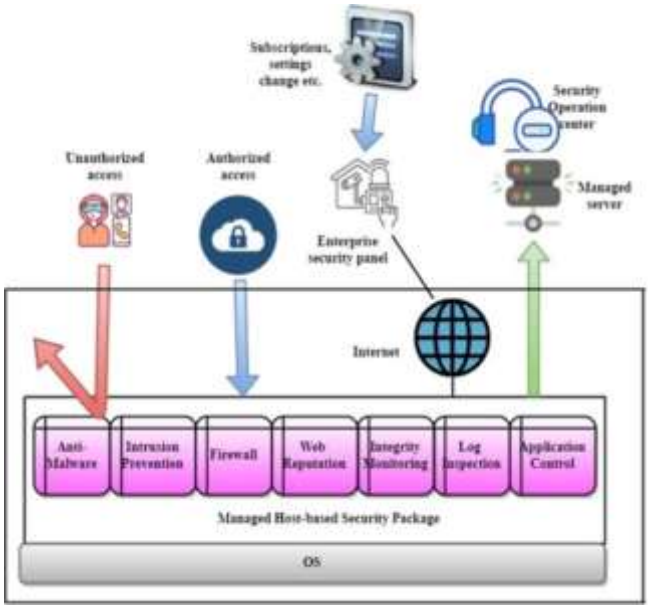

Figure 7: Host security protection package

Figure 7 illustrates how an anti-malware program retains a file in a sandbox for further examination and analysis. Viruses and other malicious files will be deleted immediately, while genuine items may remain but be closely watched. A computer's anti-malware software instantly identifies and removes harmful software from its operating system. An intrusion prevention system (IPS) is a piece of hardware or software used to protect a computer system against hackers. If this happens, it will report, block, or eliminate it. The barriers and other internet filtering appliances analyze network activities according to the organization's predetermined safety procedures. Firewalls are used to prevent unauthorized access to encrypted networks from the internet. Protecting against malicious websites is made easier with the help of Web Reputation. Web Reputation uses the Trend Data Online security registry to assess the risk associated with every URL queried. With Web Reputation Filtering, new websites are compared to recognized sites and blocked from access if they include harmful code, many of which might leave the device useless. They may lose the apps and data in certain instances.

$$Y = \dot{a}\langle p_{-1}\rangle \uparrow \frac{1}{2}(u_2) * \sqrt[2]{a^2 - p^2} \tag{13}$$

Equation 13 gives Y for anti-malware, a for intrusion prevention, p for firewall, u for web reputation. Many other types of malwares go by antivirus, yet the phrase implies that it solely defends against computer viruses. Anti-malware software can detect complex malware, such as zero-day attacks, while antivirus programs can thwart traditionally threats. The System Integrity Monitoring job aims to keep track of changes made to the files and directories inside the defined monitoring scopes. A security breach on the protected server can be detected using this task. The

Doi: https://doi.org/10.54216/FPA.150220
Received: August 08, 2023 Revised: December 16, 2023 Accepted: April 09, 2024

Integrity Monitoring protection module monitors files and essential system regions like the Windows registry for suspicious behavior [43]. However, Integrity Monitoring cannot prevent or reverse any modifications to the system. The deep security log inspection module allows for gathering and analyzing operating system and application logs for security events. Security incidents hidden in a sea of log entries are easier to find with Log Inspection rules in place. All computerized applications, including hardware, software, and manual processes, are subject to general controls, forming an overall control environment. Application controls are the individual settings for each automated program.\

$$H = \iiint r * l_2" \; cos \; cos \; r^2 \; [h_2] - l^2 \mp h_r^{-1} \tag{14}$$

Equation 14 denotes H for integrity monitoring, r for log inspection, l for application control, and h for the internet. Application control forbids or restricts unauthorized software usage, protecting sensitive information from compromise. The fullness and validity checks, identification and authentication, authorization, input controls, and forensic controls are all a part of the application control. When someone gets access to a website, application, server, service, or other systems without authorization, they have unauthorized access [45]. These warnings serve as a deterrent to hackers trying to get into a safe or secret system. When a user repeatedly fails to log into their account, the account may be locked. The operating system assesses whether or not a process has the authority to run on this system via access authorization. Security for an operating system may be provided by using two-factor authentication. Protecting both infrastructure and applications is the goal of enterprise security solutions. Enterprise security architecture is a kind of risk management geared at companies with many users dispersed across several locations. The security operation center (SOC) is responsible for various tasks, including continuously monitoring and improving the organization's safety posture and the prevention, identification, analysis, and response to cyber-attacks. Windows-based servers often act as the management server, in charge of all policy generation, storage, and installation. A single management server may handle a dozen or more enforcement points. Each of them may have its own set of rules. The host-based packet audit guards the system against known and new attacks on weaknesses in OS, middleware, applications, etc., networks. Its intrusion detection/intrusion prevention features keep an eye out for any suspicious communication that comes through.

$$W = \sqrt[4]{b} + (c)^2 \leftrightarrow \int \left\{ b^{-1} * \frac{d^2}{c} \right\} \cap c_d \tag{15}$$

Equation 15 refers to W for host-based security, b for unauthorized access, d for a managed server, c for accuracy in security protection. It analyses a whole security ecosystem to discover suspicious behavior that might compromise the network. Detection of a threat requires immediate mitigation measures to stop it before exploiting any existing vulnerabilities. The following figure 6 explains the mathematical function of the method as mentioned above.

Algorithm 1: ICT-SC-HS

```
FUNCTION secureSystemAndNetwork()
// Step 1: Antivirus Scanning
   files = downloadFiles()
   FOR each file IN files
      IF antivirusScan(file) THEN openFile(file)
      ELSE quarantineFile(file) END IF
   END FOR
 // Step 2: Frequent Scans
   IF frequentScansEnabled() THEN
      scheduleDailyScans()    END IF
 // Step 3: Anti-malware Protection
   IF antiMalwareEnabled() THEN  enableAntiMalware()
   END IF
// Step 4: Smart City Structure,
   displaySmartCityStructure()
// Step 5: Overall Structure of ICT-SC-HS
   displayOverallStructure()
```


Doi: https://doi.org/10.54216/FPA.150220
Received: August 08, 2023 Revised: December 16, 2023 Accepted: April 09, 2024

```
    // Step 6: Safety Device
    IF suspiciousActivityDetected() THEN  soundAlarm()
    END IF
    // Step 7: Smart City Technology    optimizeTrafficFlow()
    // Step 8: Routing and Encryption     configureRouting()
    IF needAccessToEncryptedData() THEN
       provideAccess()    END IF
    // Step 9: Mathematical Representation
    displayMathematicalRepresentation()
    // Step 10: Information Leakage
       protectAgainstDataLeakage()
    // Step 11: Smart Mobility   implementSmartMobility()
    // Step 12: Access Controls   implementAccessControls()
    // Step 13: Network Attacks   detectNetworkAttacks()
    // Step 14: Data Analytics
    analyzeDataForSecurityVulnerabilities()
    // Step 15: Heterogeneous Networks
    manageHeterogeneousNetworks()
    // Step 16: Scalability       ensureScalability()
    // Step 17: Smart Sensors   implementSmartSensors()
    // Step 18: Robustness      ensureSystemRobustness()
    // Step 19: Feature Extraction
       performFeatureExtraction()
    // Step 20: Anomaly Detection    detectAnomalies()
    // Step 21: Security Alarm    activateSecurityAlarms()
    // Step 22: Network Traffic Analysis
        analyzeNetworkTraffic()
    // Step 23: Signature Verification   verifySignatures()
    // Step 24: Pattern Signatures
       applyPatternSignatures()
   // Step 25: Host Security Protection Package
    displayHostSecurityProtectionPackage()
   // Step 26: System Integrity Monitoring
    monitorSystemIntegrity()
   // Step 27: Deep Security Log Inspection
    inspectSecurityLogs()
   // Step 28: Application Controls
    implementApplicationControls()
   // Step 29: Unauthorized Access
    detectUnauthorizedAccess()
   // Step 30: Two-Factor Authentication
    implementTwoFactorAuthentication()
   // Step 31: Enterprise Security Solutions
    deployEnterpriseSecuritySolutions()
   // Step 32: Security Operation Center
    manageSecurityOperations()
   // Step 33: Host-Based Packet Audit
    performHostBasedPacketAudit()
   // Step 34: Detect and Mitigate Threats
    IF threatDetected() THEN  takeMitigationMeasures()
    END IF
END FUNCTION
```

The article offers a thorough strategy for protecting computer systems and networks from malicious cyber activity, focusing on the role that technology and best practices may play. Antivirus software, routine scanning, and malware detection are highlighted for their protective role against cyber-attacks and technological exploitation. This approach examines the importance of smart cities in urban planning and environmental sustainability, focusing on optimizing traffic flow to reduce

Doi: https://doi.org/10.54216/FPA.150220
Received: August 08, 2023 Revised: December 16, 2023 Accepted: April 09, 2024

congestion. The proposed system, ICT-SC-HS, collects data from the Internet of Things and tracks network activity to identify and stop cyberattacks. Data security is discussed alongside precautions, energy efficiency, alternative routes, and encryption. Information leakage, access controls, data-driven security, scalability, robustness, evaluating host networks, host security attacks, smart sensor technology, anomaly detection, signature verification, misinformation campaigns, network congestion, security operations centres, application controls, unauthorized access, account locking, enterprise security solutions, and host-based packet audits are also discussed.

4. Experiment on Host Security Protection

The proposed model utilizes the dataset BETH dataset. https://www.kaggle.com/datasets/katehighnam/beth-dataset [40]. Anomalous data and changes in distribution are unavoidable when applying ML models to the actual world. When considering cyber security, it's important to note that defensive and adversary progress contributes to these anomalies and shifts in datasets. Therefore, deployed defensive systems' performance, security, and lifespan depend on creating robust models to bear the cost of crucial system failure. As the first cybersecurity dataset, the BPF-extended tracking honeypot (BETH) is used to benchmark robustness and uncertainty. Security problems that network evaluations can recognize can only be discovered through host system security evaluations. The company's operating systems and applications are examined for security problems at the operating system and application level. Scanning hosts for vulnerabilities using host-based vulnerability scanners is an excellent way to understand better how a system is configured and what patches have been applied. A host-based security system provides intrusion prevention services, including behavioural and signature protection. Workstation firewall security is provided via host-based protection, which filters between the host computer and the network. A host-based firewall is an installed program on a particular host that restricts internet traffic just for that host. Keeping a host clean and preventing infected ones from transmitting malware to other computers is possible.

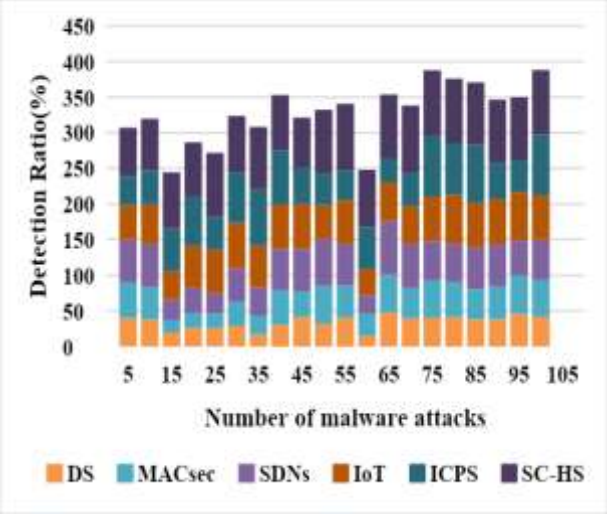

Figure 8: Malware detection from different attacks

Figure 8 represents the antivirus software that analyses a program's signature to see whether it contains certain malware. The signatures of viruses and worms are stored in enormous databases by commercial antivirus software, which scans every file for these signatures. Static strings aren't the only thing antivirus can detect, and it's not limited to only infections. When browsing for known malware, a heuristic analysis may discover a significant proportion of unknown malware with remarkable accuracy. Host-based detection systems may defend systems in real-time by checking for abnormal activity and signals of an attack in the design and responding accordingly.

Doi: https://doi.org/10.54216/FPA.150220
Received: August 08, 2023 Revised: December 16, 2023 Accepted: April 09, 2024

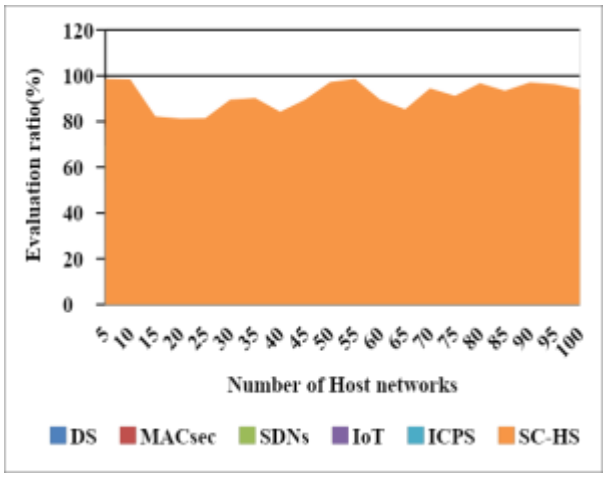

Figure 9: Evaluation of host networks

Figure 9 illustrates the access points linked directly to one another are uncommon. However, knowing how a Switch or Router supports multi-host connectivity or multi-network communication is critical to this understanding. For each host for the network, the portion of the Internet address they assign is unique. The network portion of each host's address must be individual, but the host portion must be the same for each host on their network. Subnets are identified by network addresses, and host addresses are placed on a computer or a device's subnet.

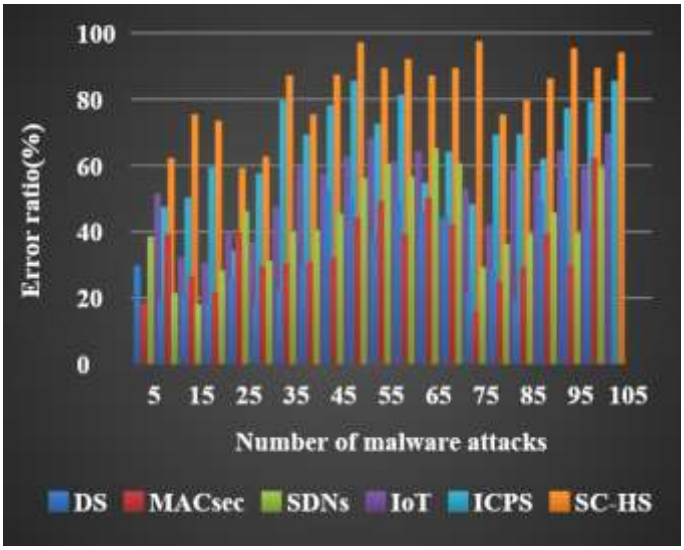

Figure 10: Absolute errors of security analysis

Figure 10 shows that smart cities' efficient operation depends on correct data; a city might be halted if that data is compromised. Traffic control systems, for example, might be used to produce traffic delays or collisions. Subways might be shut down, or water supplies could be poisoned, name a few more dangers. Web servers commonly route HTTP requests to specific virtual hosts depending on the value provided in the Host header during the request submission process. An attacker may poison the web server's cache by supplying erroneous data without performing header value validation. A stock's predicted return and risk may be established using security analysis, which helps investors make sensible decisions about a stock's value.

Doi: https://doi.org/10.54216/FPA.150220
Received: August 08, 2023 Revised: December 16, 2023 Accepted: April 09, 2024

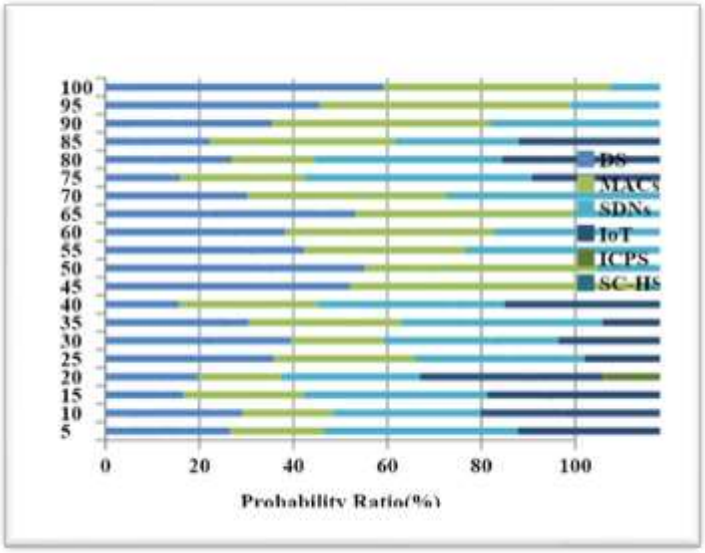

Figure 11: Probability of network protection

Figure 11 explains that the edges present or absent in the past may be used to calculate a network's probability matrix. For example, individuals in a social network are not linked to each other with equal randomness. Directed graphical models like the host network may represent a portion of the independent connections in a joint probabilistic model. A probability distribution for the related random variables is attached to each node in the network. In a computer network, two or more computers are linked by a wired or wireless connection. A two-computer network connected by a thread is the most basic network.

Table 2: Accuracy Of Security

Number of hosts	DS	MACsec	SDNs	IoT	ICPS	SC-HS
2	20.5	29.5	39.75	59.6	64.6	73.2
4	18.3	25.6	38.9	65.3	48.5	79.6
6	24.3	47.3	36.4	78.7	62.1	80.3
8	38.6	46.3	64.6	63.2	45.7	81.2
10	42.3	59.3	79.3	58.8	70.2	91.4
12	37.3	42.2	57.7	52.9	38.3	83.5
14	36.2	55.6	70.2	67.3	53.2	75.2
16	38.3	46.9	53.8	45.9	28.2	73.3
18	29.2	49.1	62.9	76.7	69.8	79.9
20	55.6	41.9	62.3	58.6	37.5	81.4
22	32.3	54.5	42.9	73.2	59.7	90.4
24	45.3	60.4	63.7	77.6	65.2	96.2
26	42.3	59.3	69.6	80.3	76.3	92.5
28	34.6	45.5	70.5	76.2	53.4	97.3
30	56.3	69.4	79.4	62.4	73.4	91.2
32	53.3	58.3	60.6	73.5	63.5	89.7
34	40.8	46.3	53.2	80.2	77.8	93.8
36	34.6	45.5	52.4	70.3	67.2	95.4
38	46.9	58.3	62.1	70.9	67.5	79.2

Doi: https://doi.org/10.54216/FPA.150220
Received: August 08, 2023 Revised: December 16, 2023 Accepted: April 09, 2024

40	36.4	45.2	57.2	71.4	69.5	82.7

Table 2 gives the accuracy that the data is accurate and error-free. Accuracy is critical to the quality of information, which is determined by timeliness, completeness, relevance, and the ease with which the intended audience can comprehend the data. It's common knowledge that a model's accuracy is measured in the percentage of accurate forecasts to the total predictions. However, a model's efficiency cannot be determined by its accuracy. When data is uneven, it is not guaranteed that the model will effectively detect anomalies. Even if we have a well-balanced dataset, we still need to consider the metrics, which might aid in selecting the various approaches. System administrators can follow changes to essential files and directories on their computers with the help of a host-based network monitoring system. As a host-based protection system does not need to search for patterns, merely changes within a specified set of criteria, this is one of its benefits.

Table 3: Host Security Protection from Malware Attacks

Number of hosts	DS	MACsec	SDNs	IoT	ICPS	SC-HS
5	25.2	39.3	25.3	48.8	60.2	78.4
10	35.1	48.2	62.7	42.9	63.3	71.5
15	15.5	23.8	42.3	60.1	69.3	78.4
20	28.3	22.9	38.2	56.9	69.5	75.7
25	36.2	20.3	40.4	52.6	67.1	81.3
30	25.2	36.5	49.8	64.4	70.3	79.4
35	17.9	26.7	40.5	57.3	69.3	83.4
40	32.3	48.3	53.6	67.3	79.3	85.2
45	45.3	36.3	52.6	69.2	79.7	92.2
50	40.3	53.3	38.3	57.8	74.2	89.4
55	35.2	40.2	57.7	65.9	75.3	93.5
60	23.9	38.9	25.3	76.1	70.3	80.4
65	49.6	65.3	45.3	63.8	74.2	89.4
70	29.5	42.2	32.7	59.9	77.3	93.5
75	40.5	52.2	55.4	62.7	85.6	97.2
80	43.3	59.2	53.2	69.2	72.5	90.4
85	18.2	32.3	48.6	62.3	81.3	88.2
90	38.2	46.3	59.6	63.2	50.7	88.2
95	26.2	53.3	39.3	67.8	44.2	89.4

Doi: https://doi.org/10.54216/FPA.150220
Received: August 08, 2023 Revised: December 16, 2023 Accepted: April 09, 2024

100	41.9	52.2	55.4	62.7	85.6	90.2

Table 3 presents the environmental awareness that helps malware samples discover more about the operating system they are attempting to attack. Malware may evade detection by signature-based antivirus software by confounding automated instruments, which is the second method of evasion. The expression system functionality applies to a cyber-physical system that enables integrated management of all components, employing various technology tools that help assemble and analyze data to achieve efficiency, sustainability, productivity, and safety goals. With the smart pavement road system, vehicles' locations and road conditions may be tracked in real-time using high-resolution cameras embedded in the pavement. These embedded technologies may detect accidents, and emergency personnel can be alerted automatically. The provided results provide a high-level overview of a cybersecurity study performed on the BETH dataset, with attention paid to various aspects of security such as malware detection, host network evaluation, absolute errors in security analysis, probability of network security, accuracy classification, and the enhancement of host security protection from malware attacks. Antivirus software's ability to analyze program signatures and identify malicious software is depicted in Figure 7. It stresses that heuristic analysis is essential and that depending on static signatures alone is insufficient when identifying unknown malware. Host-based detection systems are also highlighted for real-time defense against abnormal activity and attack signals. Figure 8 shows how crucial it is to comprehend host network connectivity. Knowledge of how switches and routers support multi-host connectivity is highlighted, as it is noted that direct links between access points are uncommon. Subnets and private host addresses within a network are also covered in detail. The importance of reliable data in the smooth functioning of smart cities is illustrated in Figure 9. Data breaches are highlighted as a serious threat to infrastructure, including transportation networks, utilities, and public health. Data validation and security analysis are crucial to preserving the system's reliability. The idea of deriving the probability matrix of a network from its past edge data is presented in Figure 10. It explains that not all network links are created randomly; therefore, directed graphical models can accurately depict unrelated links. The discussion includes some rudimentary information on how computer networks work. The success rates of various numbers of hosts in performing security-related tasks are listed in Table 1. It recognizes that accurate data is essential yet only one of the factors in a model's success. Metrics are discussed, and the need to do so is emphasized, mainly when dealing with unbalanced datasets. Also discussed is how host-based network monitoring devices function. Table 2 shows some numbers about how host security has improved in response to malware. It explains why virus evasion solutions need to consider the surrounding environment. The importance of integrated data analysis for efficacy and safety in cyber-physical systems is introduced, along with the idea of system functionality. In summary, these findings highlight the multidimensional nature of cybersecurity research and the significance of precision, data analysis, and real-time defenses. The importance of security in cyber-physical systems and smart cities is also discussed. To fully grasp the implications of these trials, further information is needed regarding the study's methodology, datasets, and individual results.

5. Conclusion

The increasing connectivity of smart cities, driven by advancements in communication technologies such as 5G and self-driving cars, creates new opportunities for cybercrime. Host-based security (HS) offers a critical line of defence against these threats, protecting individual devices within the smart city infrastructure. The proposed approach, ICT-enabled Smart City based Host security (ICT-SC-HS), leverages multi-level data fusion to achieve significant improvements in host-based malware detection, network evaluation, and security analysis. This translates to a more secure and resilient smart city environment, allowing citizens to thrive and IT administrators to focus on strategic priorities. With a demonstrated 72.1% malware detection rate across various attack scenarios, 69.7% accuracy in host network evaluation, and improved performance in other key metrics, ICT-SC-HS holds significant promise for safeguarding smart cities from cyber threats. We are actively expanding our research to encompass a wider range of potential threats, further enhancing the security of smart cities for the future.

Doi: https://doi.org/10.54216/FPA.150220
Received: August 08, 2023 Revised: December 16, 2023 Accepted: April 09, 2024

Acknowledgement:

The authors would like to University of Technology, Baghdad, Iraq, Universiti Teknikal Malaysia Melaka (UTeM), Universitas Alma Ata for providing the facilities and support for this research. All authors read and approved the final manuscript.

Funding: "This research received no external funding"

Conflicts of Interest: "The authors declare no conflict of interest."

References

[1] Darch Abed Dawar, A. (2024). Enhancing Wireless Security and Privacy: A 2-Way Identity Authentication Method for 5G Networks. International Journal of Mathematics, Statistics, and Computer Science, 2, 183–198. https://doi.org/10.59543/ijmscs.v2i.9073

[2] Lata, S., & Singh, D. (2022). Intrusion detection system in cloud environment: Literature survey & future research directions. *International Journal of Information Management Data Insights*, *2*(2), 100134.

[3] Mahbub, M. (2020). Progressive researches on IoT security: An exhaustive analysis from the perspective of protocols, vulnerabilities, and preemptive architectonics. Journal of Network and Computer Applications, 168, 102761

[4] Noor, Z., Hina, S., Hayat, F., & Shah, G. A. (2023). An Intelligent Context-Aware Threat Detection and Response Model for Smart Cyber-Physical Systems. Internet of Things, 100843.

[5] Kure, H. I., Islam, S., & Mouratidis, H. (2022). An integrated cyber security risk management framework and risk predication for the critical infrastructure protection. *Neural Computing and Applications*, *34*(18), 15241-15271.

[6] Noor, Z., Hina, S., Hayat, F., & Shah, G. A. (2023). An Intelligent Context-Aware Threat Detection and Response Model for Smart Cyber-Physical Systems. *Internet of Things*, 100843.

[7] Lehmann, D., Kinder, J., & Pradel, M. (2020). Everything Old is New Again: Binary Security of {WebAssembly}. In 29th USENIX Security Symposium (USENIX Security 20) (pp. 217-234).

[8] Zhang, H., Wang, B., Yu, X., Li, J., Shang, J., & Yu, J. (2020). Carbon dots in porous materials: host–guest synergy for enhanced performance. Angewandte Chemie, 132(44), 19558-19570.

[9] Bjørkhaug, I. (2020). Revisiting the refugee–host relationship in Nakivale Refugee Settlement: A dialogue with the Oxford Refugee Studies Centre. Journal on Migration and Human Security, 8(3), 266-281.

[10] Labuda, P. I. (2020). UN Peacekeeping as intervention by invitation: host state consent and the use of force in Security Council-mandated stabilisation operations. Journal on the use of force and international law, 7(2), 317-356.

[11] Monebhurrun, N. (2020). Diligentia quam in suis as a Technique for a Contextual Application of the Full Protection and Security Standard: Considering the Level of Development of Host States in International Investment Law. African Journal of International and Comparative Law, 28(4), 596-611.

[12] Ou, Y., Zhou, W., Zhu, Z., Ma, F., Zhou, R., Su, F., ... & Liang, H. (2020). Host Differential Sensitisation toward Color/Lifetime-Tuned Lanthanide Coordination Polymers for Optical Multiplexing. Angewandte Chemie International Edition, 59(52), 23810-23816.

[13] Rao, P. M., & Deebak, B. D. (2022). Security and privacy issues in smart cities/industries: Technologies, applications, and challenges. Journal of Ambient Intelligence and Humanized Computing, 1-37.

[14] Manogaran, G., Alazab, M., Shakeel, P. M., & Hsu, C. H. (2021). Blockchain assisted secure data sharing model for Internet of Things based smart industries. IEEE Transactions on Reliability, 71(1), 348-358.

[15] Stergiopoulos, G., Lygerou, E., Tsalis, N., Tomaras, D., & Gritzalis, D. (2020). Avoiding Network and Host Detection using Packet Bit-masking. In ICETE (2) (pp. 52-63).

[16] Chen, X. (2020). Pathogens which threaten food security: Puccinia striiformis, the wheat stripe rust pathogen. Food Security, 12(2), 239-251.

Doi: https://doi.org/10.54216/FPA.150220
Received: August 08, 2023 Revised: December 16, 2023 Accepted: April 09, 2024

[17] Neef, A. (2020). Legal and social protection for migrant farm workers: lessons from COVID-19. Agriculture and Human Values, 37(3), 641-642.
[18] Zhang, J. (2022, April). Design of Campus Network Security System Based on Network Information Security. In 2022 IEEE Asia-Pacific Conference on Image Processing, Electronics and Computers (IPEC) (pp. 1194-1197). IEEE.
[19] Jiang, J. (2021, May). Research on Application of Idc Virtualization Security Technology Based on Host Whitelist Protection. In Journal of Physics: Conference Series (Vol. 1915, No. 3, p. 032011). IOP Publishing.
[20] Abd El-Latif, A. A., Abd-El-Atty, B., Elseuofi, S., Khalifa, H. S., Alghamdi, A. S., Polat, K., & Amin, M. (2020). Secret images transfer in cloud system based on investigating quantum walks in steganography approaches. Physica A: Statistical Mechanics and its Applications, 541, 123687.
[21] Alqahtani, H., Sarker, I. H., Kalim, A., Hossain, M., Md, S., Ikhlaq, S., & Hossain, S. (2020, March). Cyber intrusion detection using machine learning classification techniques. In International Conference on Computing Science, Communication and Security (pp. 121-131). Springer, Singapore.
[22] McLaughlin, M. (2020). State-Owned Enterprises and Threats to National Security Under Investment Treaties. Chinese Journal of International Law, 19(2), 283-327.
[23] Mombeuil, C. (2020). An exploratory investigation of factors affecting and best predicting the renewed adoption of mobile wallets. Journal of Retailing and Consumer Services, 55, 102127.
[24] Mahbub, M. (2020). Progressive researches on IoT security: An exhaustive analysis from the perspective of protocols, vulnerabilities, and preemptive architectonics. Journal of Network and Computer Applications, 168, 102761.
[25] Geffre, A. C., Gernat, T., Harwood, G. P., Jones, B. M., Gysi, D. M., Hamilton, A. R., ... & Dolezal, A. G. (2020). Honey bee virus causes context-dependent changes in host social behavior. Proceedings of the National Academy of Sciences, 117(19), 10406-10413.
[26] Tian, R., Yang, Z., & Shao, Q. (2020). Effects of host country resource endowment and labor cost on China's investment in overseas cultivated land. Environmental Science and Pollution Research, 27(36), 45282-45296.
[27] Yang, P., Xiong, N., & Ren, J. (2020). Data security and privacy protection for cloud storage: A survey. IEEE Access, 8, 131723-131740.
[28] Li, Y., Yao, S., Zhang, R., & Yang, C. (2021). Analysing host security using D-S evidence theory and multisource information fusion. International Journal of Intelligent Systems, 36(2), 1053-1068.
[29] Hauser, F., Schmidt, M., Häberle, M., & Menth, M. (2020). P4-MACsec: Dynamic topology monitoring and data layer protection with MACsec in P4-based SDN. IEEE Access, 8, 58845-58858.
[30] Zaballa, E. O., Franco, D., Zhou, Z., & Berger, M. S. (2020, February). P4Knocking: Offloading host-based firewall functionalities to the network. In 2020 23rd Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN) (pp. 7-12). IEEE.
[31] Gassais, R., Ezzati-Jivan, N., Fernandez, J. M., Aloise, D., & Dagenais, M. R. (2020). Multi-level host-based intrusion detection system for internet of things. Journal of Cloud Computing, 9(1), 1-16.
[32] Liu, J., Zhang, W., Ma, T., Tang, Z., Xie, Y., Gui, W., & Niyoyita, J. P. (2020). Toward security monitoring of industrial cyber-physical systems via hierarchically distributed intrusion detection. Expert Systems with Applications, 158, 113578.
[33] Oyewole, S. (2020). Civil-military Relations: Conflict and Cooperation between Military Bases and Host Communities in Nigeria. African Security, 13(4), 353-379.
[34] Sun, P. (2020). Security and privacy protection in cloud computing: Discussions and challenges. Journal of Network and Computer Applications, 160, 102642.
[35] Rahman, M. T., Tajik, S., Rahman, M. S., Tehranipoor, M., & Asadizanjani, N. (2020, December). The key is left under the mat: On the inappropriate security assumption of logic locking schemes. In 2020 IEEE International Symposium on Hardware Oriented Security and Trust (HOST) (pp. 262-272). IEEE.
[36] Al-Otum, H. M. (2020). Secure and robust host-adapted color image watermarking using inter-layered wavelet-packets. Journal of Visual Communication and Image Representation, 66, 102726.
[37] Dubey, A., Cammarota, R., & Aysu, A. (2020, December). Maskednet: The first hardware inference engine aiming power side-channel protection. In 2020 IEEE International Symposium on Hardware Oriented Security and Trust (HOST) (pp. 197-208). IEEE.
[38] Haas, S., Sommer, R., & Fischer, M. (2020, September). Zeek-osquery: Host-network correlation for advanced monitoring and intrusion detection. In IFIP International Conference on ICT Systems Security and Privacy Protection (pp. 248-262). Springer, Cham.

Doi: https://doi.org/10.54216/FPA.150220
Received: August 08, 2023 Revised: December 16, 2023 Accepted: April 09, 2024

[39] Lee, J. M., & Hong, S. (2020). Keeping host sanity for security of the SCADA systems. IEEE Access, 8, 62954-62968.
[40] https://www.kaggle.com/datasets/katehighnam/beth-dataset
[41] M. El El-Taie and A. Y. Y.Kraidi, "Blockchain Meets Edge Intelligence for Smart Cities Sustainability: An Insightful Review and Prospective Analysis," J. Cybersecurity Inf. Manag., vol. 12, no. 1, pp. 50–61, 2023, doi: 10.54216/JCIM.120105.
[42] A. Z. Abualkishik and R. Almajed, "Managing Information Security Risks in the Age of IoT," J. Cybersecurity Inf. Manag., vol. 11, no. 01, pp. 30–37, 2023, doi: 10.54216/JCIM.110103.
[43] A. Aziz, S. Mirzaliev, and Y. Maqsudjon, "Real-time Monitoring of Activity Recognition in Smart Homes: An Intelligent IoT Framework," J. Intell. Syst. Internet Things, vol. 10, no. 1, pp. 76–83, 2023, doi: 10.54216/JISIoT.100106.
[44] F. V. Naranjo, S. M. Vivar, E. J. Arias, and R. Atassi, "Early Energy Consumption Prediction as a Key Element in Smart City Sustainability," J. Intell. Syst. Internet Things, vol. 11, no. 1, pp. 12–20, 2024, doi: 10.54216/JISIoT.110102.
[45] A. Mosa and A. Abdelaziz, "A Survey on Web Service Discovery Approaches," Fusion Pract. Appl., vol. 5, no. 2, pp. 53–60, 2021, doi: 10.54216/FPA.050202.
[46] A. A. Elngar, K. M. Sagayam, and A. A. Elngar, "Augmenting security for electronic patient health record (ePHR) monitoring system using cryptographic key management schemes," Fusion Pract. Appl., vol. 5, no. 2, pp. 42–52, 2021, doi: 10.54216/FPA.050201.
[47] M. El El-Taie and A. Y. Y.Kraidi, "A Deep Learning Framework for Securing IoT Against Malwares," J. Cybersecurity Inf. Manag., vol. 11, no. 01, pp. 38–46, 2023, doi: 10.54216/JCIM.110104.

Doi: https://doi.org/10.54216/FPA.150220
Received: August 08, 2023 Revised: December 16, 2023 Accepted: April 09, 2024