Available online www.jsaer.com

***Journal of Scientific and Engineering Research*, 2019, 6(6):191-201**

Research Article

ISSN: 2394-2630
CODEN(USA): JSERBR

Invisible Security

Anvesh Gunuganti

maverickanvesh@gmail.com

Abstract: In bridging the prevalence of virtual threats in cybersecurity, this research aims to study hidden security measures and their efficiency, solidity, and outcome. Invisible security is very effective in providing good security to the system and, at the same time, does not cause much annoyance to the users. The methodology of the work is based on a literature review and technical case study analysis that includes such topics as investors' behavior in Finland, the NHSnet, and wireless tire pressure monitoring systems. Therefore, the findings stress that security innovations based on transparency and obscurity make security more robust without disrupting users' actions. Behavioral analytics can be very effective when detecting anomalies and aid in breach detection and prevention. Data security, encryption methods, and constant updates are significant for data protection and system security. The following is a list of operational recommendations that may be implemented to enhance the security of any system in the foreseeable future: Incorporation of behavioral studies ADA Consolidation of encryption of data Secure wireless systems. Further research should be devoted to improving behavioral analysis and data protection, further considering wireless security issues, and finally, creating solutions adjusted to users' needs. Thus, this study establishes the aptitude of invisible security in enhancing the safety of computer systems in the context of a user-friendly experience.

Keywords: Invisible security, Behavioral analytics, Data encryption, Wireless security, Cybersecurity

Introduction

With the increasing frequency and sophistication of cyber attacks, it has become increasingly important to find new ways to protect secure data and applications from cyber threats while ensuring usability and accessibility. Invisible security is an innovative approach in cybersecurity as it implies utilizing security tools that become a part of the user interface and are not known by the end user [1]. It includes features such as background encryption and threat identification, which do not complicate the process and guarantee your computer's security. Information technology security goals seek to provide the highest security to the systems while at the same time not hampering regular operations or reducing speed, and this is what invisible security seeks to achieve.

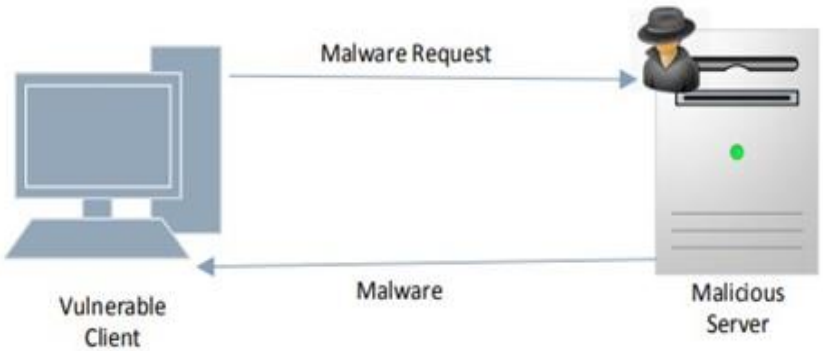

Fig. 1: Client to client Cyber attack [12]

History and Evolution of Security Approaches

The classification of security approaches can be dated back to the historical development of computers, where there was a more manual security measure, which were detective and mostly performed after something bad had occurred [2]. The first generation of computer security was practiced during the 1960s and 1970s, when the main concern was physical security and password protection to control computer system access. These methods were generally crude and depended much on the care and knowledge of the persons as users or administrators. The recent rise of the internet, especially towards the last decades of the twentieth century and the first quarters of the twenty-first century, also introduced innumerable and significantly more intricate forms of threats from cyberspace [3]. During this period, security management was also stepped up by developing advanced technologies in the detection of invaders, otherwise known as IDS and IPS, through which intrusions could be detected and a real-time response initiated. These systems were supported by encryption technologies, meaning that even if data transmitted in the respective systems was intercepted, the information was encrypted hence safe. Today, the emphasis is placed on including security as an intrinsic component of systems and applications. This shift is under the understanding that reactive measures that depend on the users cannot address modern complex and persistent threats. Invisible security, therefore, can be held to be the epitome of this evolution, wherein security elements, including background encryption, automatic threat identification, and even machine learning algorithms, among others, can run discreetly in the background. These measures are meant to be background, and they should not in any way hinder or even inform users that security processes are in the background performing their work. Another factor of invisible security is that protective measures must be integrated without any conflict with the user's ongoing tasks and should not act as a resource hog [4].

A. Significance of Invisible Security in Modern Cybersecurity

Impact of Invisible Security on Enhancing Cybersecurity

Invisible security still has a major role in enterprise cyber security as it's a proactive approach that can run twenty-four hours a day. Because they act covertly, such security measures can spot threats and act against them before much harm can be done. It secures the position of an organization by increasing its protection and making it ready to prevent newly developing threats. Thus, one of the major advantages of invisible security is that it does not burden the IT and security staff. Conventional physical security solutions usually need much vigilance and interfere with delicate security processes, making them less efficient regarding dedicated resources. However, invisible security adapts a variety of these functions, which frees up lots of time for IT and security professionals to investigate threats and devise new security mechanisms. Thus, the nature of invisible security also positively impacts compliance and general security performance. There are no extra layers of security that make it harder for the user to work with since working with the proposed tools is intuitive, and there is no chance people will not follow instructions. On the other hand, low-level security remains passive and quietly enforces security provisions without the user's interaction. This decreases the risk and possible mistakes made by human beings and enhances security and compliance.

Economic and Social Benefits of Invisible Security Measures

Reducing risk to the public and economy loses value since invisible security measures bring about important economic and social gains. Policies and procedures change in that they can be managed for maximum efficiency for the benefit of a firm as they help eliminate the occurrence of security breaches, hence saving the firm lots of cash in managing such incidences. Thus, when it comes to an effective cyber attack, organizations could face severe and, at many times, invaluable consequences in terms of assets' value, legal processes, and organizational reputation. From the above, it can be seen that invisible security enables organizations to cut related costs and balance their financial books by avoiding such breaches. Also, savings through consistent student experience, adding to organizational efficiency and productivity, are part of the economic gains. Often, security measures run in the background, allowing the users to experience them in practice and work uninterruptedly, thus ensuring the company's increased productivity. This is especially true now that the business world is highly competitive, and many industries require time and more efficient ways of doing business, such as the financial, healthcare, or manufacturing industries. Socially, the invisibility of security helps build confidence among users towards implementing digital systems. With the rising threat incidences of data breaches and cyber attacks, users, especially the vulnerable ones, have resorted to protecting their information. As a result, invisible security offers optimal protection while not hindering the utilization of internet services, which helps create a safer world

on the World Wide Web. This, in turn, promotes the usage of the digital environment and available services, which positively affects society and the economy. Moreover, owing to the specific characteristics of invisible security, this framework introduces less interference into the everyday use of technology products, positively affecting perceived satisfaction. These users can simply go about their daily jobs without worrying about a cornucopia of security measures to go through or dealing with slow-downs resulting from such measures. Security here is applied so that it becomes incidental to activities and use of technology and is therefore accepted by the users due to its ease of use.

B. Research Objectives and Scope

Aims and Objectives to Be Addressed

This review specifically aims at identifying and investigating the current design and application of the techniques of covert or seemingly hidden security measures that optimize the security of a computing system while at the same time minimizing the impact on the usability of the system as much as possible. Specific aims include:

• Describing the evaluation of the current state of invisible security technologies in terms of how appropriate they are in offering invisible and strong security solutions.
• Defining major principles and guidelines for creating nearly transparent security solutions.
• Examining the effects of IS on the efficiency of the targeted system and customers' satisfaction.
• Investigating the economic and social consequences of using that invisible form of security.
• Give recommendations for further research and development of the concept of invisible security.

Furthermore, this review seeks to uncover the state of the art in invisible security and to progress its research, which collectively can improve cybersecurity and users' interactions with technology in the information age.

C. Research Questions

How can invisible security measures, such as background encryption and automated threat detection, be designed to maximize user protection without compromising system performance or user experience?

Literature Review

Invisible security is one of the new modalities in the security field and is characterized by the lack of interference with systems functioning and data protection. The following collection of literature presents information on invisible security, starting from the concept of ideas to contemporary technologies. Further, understanding the concept's foundational principles and modern technologies, as well as the key elements of the invisible security strategy and the applied uses of the concept, lets us form a holistic idea of ways the security industry is changing. This review also reveals enormous economic and social values of invisible security and underscores the importance of this defense mechanism in defending today's electronic landscapes.

A. Exploration of Invisible Security from Concept to Implementation

Invisible security encompasses security solutions executed without any interactions with the end-users or a need for them to be aware of the solutions' presence. It is based on the assumption that security has to be transparent and combined, offering high levels of protection while interfering with the functionality as little as possible. Invisible security is made of diverse solutions hidden in the background, including the following elements and features: secureness encryption, threat detection, behavioral analysis, and deception technology. It describes integrating such technologies into system structures that operate them smartly and seamlessly. For instance, background encryption implies the data is encrypted and decrypted only when necessary without involving the user. Conversely, the adaptive threat detection system is a real-time monitor employing intelligent mechanisms to detect suspicious activities. Fig 2 shows the classification of securities.

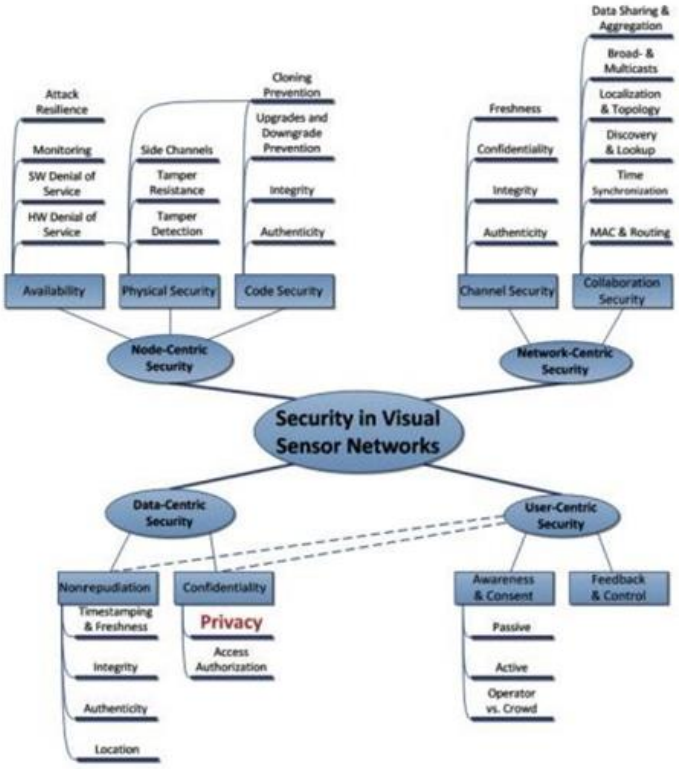

Fig. 2: Classification of security [13]

B. Key Concepts and Components

Types of Invisible Security Mechanisms

• **Behavioral Analytics:** This mechanism employs Machine Learning techniques together with data mining to analyze users' activities as it searches for signs of security threats. It means that, with the help of this approach, the system can define behavior that looks suspicious because it deviates from the conventional behavior that the system has singled out.

• **Deception Technology:** This entails using lure and snare in the network by placing traps within the systems to deceive the attackers. Seymour and Krebs describe deception technology as the creation of enticing yet fictitious objects that seem to be of value to attackers and, in the process, draw the attention of these attackers from real assets, making it possible for security teams to get early indications of an invasion.

• **Background Encryption:** The capability of encrypting data as it is generated or transmitted means that the data will only have to be encrypted once and does not need the intervention of the end users. Encryption is performed on the files on the device while transmitting over other networks and when stored.

• **Automated Threat Detection:** Software that performs network traffic analysis and system activities analysis to counter threats in a real-time manner. These systems employ signature-based and anomaly detection to detect known threats and new emerging threats on the network. Fig 4 shows the possible insider threats.

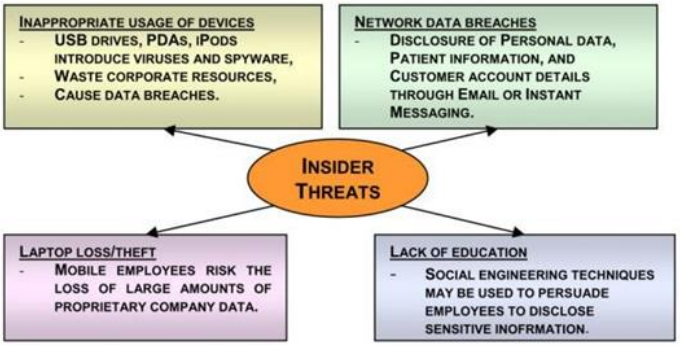

Fig. 3: Insider threats [9]

Core Principles and Technologies behind Invisible Security

The main aspects of working under invisible security concepts consist of automated approaches, integration, noninterference with end users, and threat anticipation. Technologies driving these principles include:

• **Machine Learning and AI:** It is required for assessment, forecasting, and decision-making in deviance behavior identification and security measures.

• **Encryption Technologies:** Creating options for data security and its consistency without involving the user.

• **Advanced Threat Intelligence:** Risk assessment and information exchange to counter novel threats as they are being formulated.

• **Cloud Security:** Optimizing the effectiveness of the security of distributed networks with the help of the cloud services scalability and flexibility to implement invisible security layers.

Comparison with Traditional Security Measures

In contrast, traditional security procedures point out recognizable and user-involved security methods like passwords, manual updates of applications, and virus Full Searches the users have initiated. These measures can be efficient but, at the same time, are sensitive to human mistakes and can also put a significant load on users' shoulders. On the other hand, invisible security entails a strategy to reduce dependence on users and, thus, the possibility of human mistakes. Although physical security tools can be classified as traditional security measures, invisible security is intended to be the opposite in that it will be viewed as innovative in preempting threats and neutralizing them without interfering with users' activities. It also provides better levels of security and boosts the usability and conformity levels.

Sectors Most Benefiting from Invisible Security

• **Finance:** The banking sector is a major beneficiary of invisible security since it processes and transfers huge amounts of information, and timely detection and protection against fraud are required.

• **Healthcare:** The need to safeguard the patient's information and adherence to other strict legal guidelines make healthcare one of the most appropriate industries for invisible security solutions Fig 1. It shows the organization of internet access to the Salford diabetes information system and the location of firewalls, smartcards, encryption software, and trusted third-party applications.

• **Retail:** In this regard, as e-commerce evolves, retailers employ 'invisible security' to shield customer information and payment details, hence, seamless shopping.

• **Government:** Invisible security is used by governmental institutions to keep data from leakage and to safeguard key infrastructures from cyber threats.

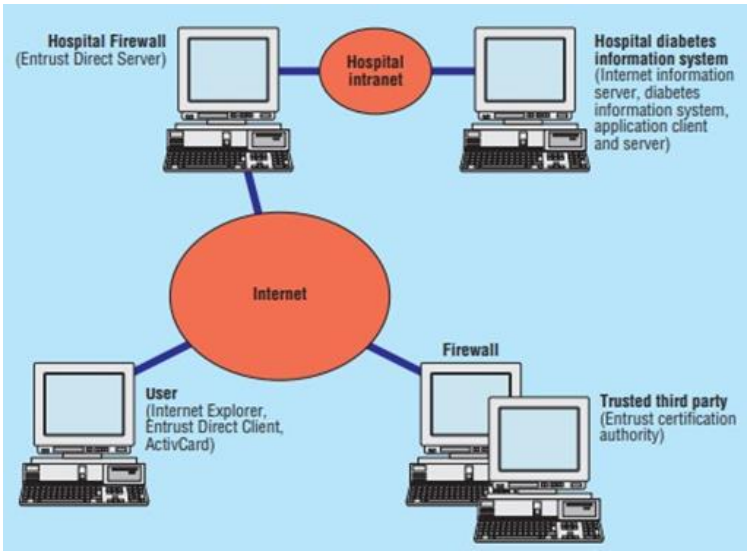

Fig. 4: Organization of Internet access to Salford diabetes information system [11]

Emerging Trends and Innovations in Invisible Security

• **Zero Trust Security Models:** Stressing on the constant validation and logging, zero trust security models correspond to the invisible security concept, as all users and devices are validated continuously.

• **AI-Driven Security:** Another trend that strengthens the invisibility concept is the integration of AI using advanced technologies for the prediction of threats and their counteraction before their realization.
• **Integration with IoT Security:** With the advancement of IoT, security is incorporated to secure many connected devices with little to no interference to their functions.
• **Edge Computing Security:** There is a growing need to secure data and applications at the network's edge, near the point of data generation, to enable real-time detection and prevention of malicious behavior.
These new trends and innovations of invisible security form the basis of future cybersecurity.

Methodology: Technical Analysis of Invisible Security

This section conducts technical analysis by analyzing entailed cases regarding the invisible security mechanisms' performance, reliability, and effectiveness. Thus, this approach enables the acquisition of information about actual deployments and their impact and the comprehensive assessment of numerous technologies in application environments. Thus, examining the implications of such specific instances will help unravel how covert security phenomena work and their function in information technology security.

A. Introduction to Technical Analysis

Explanation of Technical Analysis as a Research Method

Technical analysis is the systematic analysis of technologies and systems following the principles of empirical science and quantifiable measurements. The methodology simplifies the evaluation of performance, reliability, and effectiveness in real-life instances. In cybersecurity, technical analysis assists in comprehending these intangible security systems' functionality in real-life situations, including the consequences and performance of such systems.

Justification for Using Technical Analysis in This Review

Employing a technical approach along with case studies is imperative for gaining an unbiased look at invisible security technologies. While examples give readers an idea about specific technologies and how they work, case studies provide descriptions of the nuts and bolts. This method allows for analyzing results and performance data, critical for determining areas of excellence and used to inform further advancements in invisible security.

B. Technical Analysis Process

Detailed Description of the Technical Analysis Steps

The technical analysis process involves several steps:
• **Selection of Case Studies:** Search for examples showing the peculiarities of using invisible security mechanisms. The applications included in this paper have been selected to cover the range of application areas and show how the product has been implemented.
• **Data Collection:** Collecting exact information on each of the case studies, concrete information on the particulars of its implementation, achievement indicators, and results.
• **Evaluation Metrics:** Identification of standards for measuring the effectiveness, reliability, and performance of the system, like the accuracy of detection systems, time taken for a response, and how a system executes its functions.
• **Data Analysis:** Handling, analyzing, and interpreting the accumulated data with the help of both quantitative calculations and qualitative evaluations to find out the tendencies, patterns, and performance indicators.

Data Collection and Evaluation Procedures

Data collection is directed at acquiring information from samples selected as cases. Such as implementation reports, performance evaluations, documented users' feedback, and the results attained. In evaluation procedures, one checks the effectiveness of the mechanisms that work in the background about some parameters and compares the results with the generally accepted manifestations of safety measures.

C. Application to Invisible Security

Technical Assessment of Various Invisible Security Mechanisms

The technical assessment is based on three key case studies:

Case Study 1: Investor Behavior Analysis in Finland [8]

• **Overview:** This paper examines the characteristics of foreign and domestic investors in the Finnish stock market, particularly regarding their trading behavior and their past returns. The foreign investors are classified

as momentum investors, whereas the domestic investors, especially the households, are the contrarians. This paper concludes that portfolio performance is higher for foreign investors than for households.

• **Assessment:** The case study also explains the behavior-based approach of investment strategies regarding the investor's sophistication and performance. Although not necessarily linked to invisible security, it underscores the significance of behavioral analysis, synonymous with behavioral analytics in invisible security, in identifying any geographical abnormalities to increase protection levels.

Case Study 2: NHSnet Implementation and Security Concerns [11]

• **Overview:** This paper analyzes the British NHSnet project initiated to interconnect information systems of primary and secondary care. Some concerns were raised about protecting patients' data, the cost factor to the GP, and the issue of data access from the patient's home.

• **Assessment:** This study confirms the need for secure data management in health systems and a security shield that cannot be easily noticed due to the nature of the information in the system. The issues regarding data security and user accessibility relate to the issue solved by the invisible security technologies of meeting pervasive and reliable protective functions.

Case Study 3: Security Evaluation of Wireless Tire Pressure Monitoring Systems [10]

• **Overview:** This paper discusses the security and privacy risks of Wireless Tire Pressure Monitoring Systems in contemporary automobiles. They include eavesdropping, static identifiers, no authentications, and spoofing. The work also prescribes ways of enhancing the security of these systems.

• **Assessment:** This case indicates the threats and issues that arise with wireless systems, underlining potential threats to any wireless system, thus the necessity for unnoticeable security implementations. The conclusion confirms that the solution stresses security measures that should function behind the scenes and ensure the safety and protection of any delicate information from unauthorized access.

Evaluation of the Performance, Reliability, and Effectiveness

Each case study is evaluated based on the following criteria:

• **Performance:** Analyzing accuracy, response, system time, and influences.

• **Reliability:** Evaluating the level of conformity on identifying risks and measures for depreciation, as well as decreasing false positive cases.

• **Effectiveness:** Assessing the changes in the organization's security stance and its end-users and adherence to standards and legal requirements.

Findings and Discussion

This section provides a summary of the observation of specific seam cases and an analysis of their implications. The paper provides information about several specific kinds of invisible security technologies and the results of their usage in practice in terms of performance, reliability, and effectiveness.

A. Findings

1. Behavioral Analytics in Investor Behavior Analysis

Key Findings:

• **Behavior Patterns:** Investor behavior analysis of Finland shows that foreign investors have momentum trading as the probability ratio of buying gainers and selling losers is less than one. On the other hand, domestic investors, specifically households, hold a contrarian view where they purchase stocks that have just been beaten down.

• **Performance Differences:** Foreign investors' portfolios tend to have higher returns than domestic investors, even if adjusted by the investors' behavior. This implies that it is easier to attain higher returns through momentum-based strategies other than contrarian ones.

Discussion:

• **Relevance to Invisible Security:** The concept of dynamics evident in investors' behavior is the major reason analytics play a significant role in decision- making. Likewise, in invisible security, one can also utilize behavioral analytics to identify risks and threats by coming up with patterns of users' behavior. As mentioned, when applied correctly, momentum investing increases the overall return on investment; the same applies to behavioral analytics, and its proper application improves security breach detection and prevention.

2. NHS Net Implementation and Security Concerns

Key Findings:

• **Security and Confidentiality:** Using NHSnet creates various data security and confidentiality issues. Some patient data causes worry about the actual identity of the people who are authorized to access the patient data and others who have possibly infiltrated the system. Also, the charge that may go with connection to the NHSnet may prove prohibitive to general practitioners.

• **Accessibility Issues:** Although it is considered effective in increasing communication between primary and secondary care, NHSnet does not pertain to the availability and use of patients' data within their homes.

Discussion:

• **Relevance to Invisible Security:** The issues discussed while describing NHSnet represent invisible security. Another approach considered an element of the mechanics of invisible security technologies is data security and data confidentiality. As is evident with NHSnet, there are issues of acquiring and especially securing data; similar issues have to do with perceived security mechanisms that are usable, meaning invisible. Thus, the combination of invisibility and security adds value to data safeguarding and irretrievability in both healthcare and other industries.

3. Wireless Tire Pressure Monitoring Systems

Key Findings:

• **Vulnerabilities Identified:** Analysis of the wireless tire pressure monitoring systems provides several exposures to security, such as eavesdropping of signals, use of static identifier information to identify targets, and absence of authentication and input validation. All these vulnerabilities lead to a high privacy and security risk.

• **Experimental Evidence:** The experiments showed that with the help of specified software, one can activate warning messages at a distance. Depending on the results, wireless systems require more reliable protection.

Discussion:

• Relevance to Invisible Security: The issues in wireless tire pressure monitoring systems must be addressed to ensure proper protective measures are invisible and function in the background. These concerns can be managed well since invisible security can implement efficient encryption, authentication, and validation methods. The results of this case study demonstrate the importance of security actions that should be constant and active, without hampering systems functioning, but with the ability to counteract possible risks.

B. Discussion

The overviews of these case studies in the context of one another collectively brought to the foreground how invisible security is essential in managing multiple cybersecurity concerns. At the same time, invisible security measures can be valuable in behavioral analytics, data security, and wireless systems protection.

• **Enhanced Protection:** The idea of contextual security is always behind the application, providing constant and virtually imperceptible protection that can help improve global security. This is important to sustain good UX while at the same time having good levels of security.

• **Improved Efficiency:** This way, organizations can ensure that the implemented security measures work in the background and thus relieve the IT/security teams to work more effectively in higher-level tasks.

• **Addressing Vulnerabilities:** The potential weaknesses and issues arising in the case studies indicate that the development of further technologies of invisible security should be continued to successfully handle new threats and concerns.

In conclusion, the invisibly applied security measures demonstrate their efficiency in improving security and eliminating the drawbacks consistent with the case investigation while increasing the overall level of security and unobtrusiveness for the user.

Conclusion

A. Summary of Key Findings

This study has comprehensively looked at invisible security mechanisms through various case studies and thus offered considerable information on the functions and problems of invisible security situations. The study of investors in Finland brought out the importance of behavioral analysis in investment by realizing that foreign investors with the momentum trading system merely perform better than domestic investors within the

contrarian system. This is the same way that behavior analysis is applied in invisible security systems, where it analyzes the behaviors in a system to detect deviations from normal patterns, increasing the chances of identifying threats.

NHSnet case identified the necessity of stimulated security measures to safeguard confidential health care information. However, integrated care had been advertised as an enhancement of data exchange between primary and secondary care; issues such as costs and barriers related to the implementation had precluded general practitioners from having visible security solutions that would guarantee data protection from unauthorized access.

Also, the wireless tire pressure monitoring system assessment identified several weaknesses, including eavesdropping and spoofing, meaning that newer security technologies are needed. These identified weaknesses in these systems call for security that feature concealed security systems that can minimize these risks within the system's functionality. Altogether, these findings indicate the significance of invisible security in overcoming different cybersecurity dilemmas in an organized manner and identify the prospects for further development in this sphere.

B. Practical Recommendations for Implementing Defense Strategies

Several more specific considerations should be considered to better establish the recommended general guidelines for implementing invisible security measures. First, we need to address the issue of vulnerabilities and risks and integrate behavioral analytics to improve them. In this way, one would be able to effectively identify deviations or threats in the use of applications or the entire operational activity of an organization. This preventive strategy enables the identification of threats that have not had the chance to inflict severe harm, thus enhancing the security status of any given organization.

Second, increasing data security either by improving the methods of data encryption and authentications or by introducing new ones is a must. Security should blend with such an environment without hampering accessibility or functionality when processing the information. Strong encryption with advanced techniques and proper authentication methods can help prevent data breakage and breaches.

Third, wireless system security must be safeguarded because any weakness can become a security risk. For systems that include applications such as tire pressure monitoring, there are ways to reduce the risk, including dynamic identifiers, secure communication, and input validation. These security measures, therefore, require constant updates and frequent tests to ensure they can meet the new threats while trying to preserve system stability.

Finally, one must pinpoint usability as the foundational element for deploying more invisible security layers. It is seen that designing security solutions in such a way that the solutions work more or less invisibly does not get in the way of user activities significantly enhances user satisfaction and, accordingly, usage compliance with the security solution. This way, security and usability can be achieved in such a way that the organization is protected from possible threats, yet the users are offered environments that are easy to interact with, thereby encouraging the needed levels of trust and proper use of the protected environments.

C. Future Research Directions

Looking forward, future research should focus on addressing the following areas to further enhance ransomware defense strategies:

Advancements in Behavioral Analytics:

• Substantive research should be carried out on progressing and incorporating specific behavioral approaches to invisible security. The following examines the application of these methods and attempts to determine how such methods can be more effective in enhancing threat identification and management improvement.

Enhanced Data Security Protocols:

• Research the new encryption and authentication technologies to meet the new developing threats and hurdles. Here, efforts should be directed towards protocol research, whose main aim is to provide efficient security while at the same time not compromising the overall system or the user's ability to access the resources.

Emerging Wireless Security Challenges:

• Investigate the security of new wireless technologies and networks. Discover new effective ideas and concepts to protect wireless communication from new threats.

User-Centric Security Solutions:

• Determine the effect of security measures that cannot easily be seen on the user experience and satisfaction. Discuss the possible approaches to making security solutions sophisticated and invisible while providing maximum protection.

Also, below question directs your focus towards exploring how advanced behavioral analytics can be leveraged within invisible security frameworks to improve their ability to detect and respond to cybersecurity threats effectively. It sets the stage for investigating the practical implementation and impact of integrating behavioral analytics into security systems that prioritize user invisibility.

• **RQ:** How do different industries perceive and prioritize invisible security measures, and what factors influence their adoption and implementation?

• **Hypothesis:** This question will delve into the varying perspectives across industries regarding invisible security, exploring the factors that drive or inhibit its adoption. It allows for a comprehensive investigation into the practical implications and challenges associated with implementing invisible security measures in different organizational contexts.

Hence, invisible security is advantageous since it provides shadowing security that improves cyber security without interfering with user operations. The conclusions and suggestions made in this research give a certain impulse for further developments in this area, which considers modern problematic issues and future opportunities for enhancing protection against threats in the context of constantly growing technological innovation.

References

[1]. R. Munir, M. R. Mufti, I. Awan, Y. F. Hu, and J. P. Disso, “Detection, Mitigation and Quantitative Security Risk Assessment of Invisible Attacks at Enterprise Network,” 2015 3rd International Conference on Future Internet of Things and Cloud, Aug. 2015, doi: https://doi.org/10.1109/ficloud.2015.24.

[2]. S. Jana, A. Narayanan, and V. Shmatikov, “A Scanner Darkly: Protecting User Privacy from Perceptual Applications,” 2013 IEEE Symposium on Security and Privacy, May 2013, doi: https://doi.org/10.1109/sp.2013.31.

[3]. C. Bettini and D. Riboni, “Privacy protection in pervasive systems: State of the art and technical challenges,” Pervasive and Mobile Computing, vol. 17, pp. 159–174, Feb. 2015, doi: https://doi.org/10.1016/j.pmcj.2014.09.010.

[4]. G. Loukas, Cyber-Physical Attacks: A Growing Invisible Threat. Butterworth-Heinemann, 2015. https://books.google.com/books?hl=en&lr=&id=_OicBAAAQBAJ&oi=fnd&pg=PP1&dq=invisible+security+ measures

[5]. E. Lundin and E. Jonsson, “Anomaly-based intrusion detection: privacy concerns and other problems,” Computer Networks, vol. 34, no. 4, pp. 623–640, Oct. 2000, doi: https://doi.org/10.1016/s1389-1286(00)00134-1.

[6]. B. Schneier, Secrets and Lies: Digital Security in a Networked World. John Wiley & Sons, 2015. Available: https://books.google.com/books?hl=en&lr=&id=OT6kBgAAQBAJ&oi=fnd&pg=PR9&dq=invisible+security+measures&ots=N6sTXJpV4J&sig=hxCiXofE8BIp8Ct FZmrjtuR8RvM

[7]. S. Rathore, P. K. Sharma, V. Loia, Y.-S. Jeong, and J. H. Park, “Social network security: Issues, challenges, threats, and solutions,” Information Sciences, vol. 421, pp. 43–69, Dec. 2017, doi: https://doi.org/10.1016/j.ins.2017.08.063.

[8]. M. Grinblatt, “The investment behavior and performance of various investor types: a study of Finland’s unique data set,” Journal of Financial Economics, vol. 55, no. 1, pp. 43–67, Jan. 2000, doi: https://doi.org/10.1016/s0304-405x(99)00044-6.

[9]. K. Roy Sarkar, "Assessing insider threats to information security using technical, behavioral and organizational measures," Information Security Technical Report, vol. 15, no. 3, pp. 112–133, Aug.2010, doi: https://doi.org/10.1016/j.istr.2010.11.002.

[10]. Rouf et al., “Security and Privacy Vulnerabilities of In- Car Wireless Networks: A Tire Pressure Monitoring System Case Study.” Available: https://www.usenix.org/legacy/event/sec10/tech/full_papers/Rouf.pdf
[11]. D. W. Chadwick, "Using the Internet to access confidential patient records: a case study," BMJ, vol. 321, no. 7261, pp. 612–614, Sep. 2000, doi: https://doi.org/10.1136/bmj.321.7261.612.
[12]. S. Iqbal et al., “On cloud security attacks: A taxonomy and intrusion detection and prevention as a service,” Journal of Network and Computer Applications, vol. 74, pp. 98–120, Oct. 2016, doi: https://doi.org/10.1016/j.jnca.2016.08.016.
[13]. T. Winkler and B. Rinner, “Security and Privacy Protection in Visual Sensor Networks,” ACM Computing Surveys, vol. 47, no. 1, pp. 1–42, May 2014, doi: https://doi.org/10.1145/2545883.

Acronyms

1. RSA-Rivest-Shamir-Adleman(encryption algorithm)
2. AES-Advanced Encryption Standard
3. RaaS-Ransomware-as-a-Service
4. MBR-Master Boot Record