future internet

IMPACT FACTOR 2.8

CITESCORE 7.1

Review

Editor's Choice

Opportunities for Early Detection and Prediction of Ransomware Attacks against Industrial Control Systems

Mazen Gazzan and Frederick T. Sheldon

Special Issue

Cyber Security Challenges in the New Smart Worlds

Edited by

Dr. Agostino Forestiero and Dr. Mohamed Abd Elaziz

MDPI

https://doi.org/10.3390/fi15040144

future internet

MDPI

Review

Opportunities for Early Detection and Prediction of Ransomware Attacks against Industrial Control Systems

Mazen Gazzan [1,2] and Frederick T. Sheldon [1,*]

[1] Department of Computer Science, College of Engineering, University of Idaho, Moscow, ID 83844, USA; gazz6545@vandals.uidaho.edu or mzgazzan@nu.edu.sa
[2] College of Computer Science and Information Systems, Najran University, Najran P.O. Box 1988, Saudi Arabia
* Correspondence: sheldon@ieee.org; Tel.: +1-20829-22545

Abstract: Industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems, which control critical infrastructure such as power plants and water treatment facilities, have unique characteristics that make them vulnerable to ransomware attacks. These systems are often outdated and run on proprietary software, making them difficult to protect with traditional cybersecurity measures. The limited visibility into these systems and the lack of effective threat intelligence pose significant challenges to the early detection and prediction of ransomware attacks. Ransomware attacks on ICS and SCADA systems have become a growing concern in recent years. These attacks can cause significant disruptions to critical infrastructure and result in significant financial losses. Despite the increasing threat, the prediction of ransomware attacks on ICS remains a significant challenge for the cybersecurity community. This is due to the unique characteristics of these systems, including the use of proprietary software and limited visibility into their operations. In this review paper, we will examine the challenges associated with predicting ransomware attacks on industrial systems and the existing approaches for mitigating these risks. We will also discuss the need for a multi-disciplinary approach that involves a close collaboration between the cybersecurity and ICS communities. We aim to provide a comprehensive overview of the current state of ransomware prediction on industrial systems and to identify opportunities for future research and development in this area.

Keywords: ransomware; industrial control systems; SCADA; ransomware detection and prevention; attack likelihood prediction; situation awareness; security assessment

Citation: Gazzan, M.; Sheldon, F.T. Opportunities for Early Detection and Prediction of Ransomware Attacks against Industrial Control Systems. *Future Internet* **2023**, *15*, 144. https://doi.org/10.3390/fi15040144

Academic Editors: Agostino Forestiero and Mohamed Abd Elaziz

Received: 18 February 2023
Revised: 30 March 2023
Accepted: 3 April 2023
Published: 7 April 2023

1. Introduction

Supervisory control and data acquisition (SCADA) systems are used to control and monitor industrial processes, such as power plants, water treatment facilities, and manufacturing plants [1,2]. Due to the critical nature of these systems, cybersecurity concerns in SCADA systems are of paramount importance. Additionally, the availability of easy-to-use malware development toolkits makes it more feasible to rely on those malicious applications in many attack scenarios [3]. Some of the key concerns include system vulnerabilities, remote access, lack of security controls, lack of security awareness, and interoperability [4]. SCADA systems can contain vulnerabilities, such as unpatched software or outdated operating systems, that can be exploited by attackers to gain unauthorized access to the system [5]. Moreover, many SCADA systems can be accessed remotely, which can increase the risk of an attack [6]. For example, if an attacker can gain access to a remote access point, they could potentially take control of the system [7]. In addition, SCADA systems may not have the same level of security controls as traditional IT systems, such as firewalls or intrusion detection systems (IDS). Operators or maintenance personnel may not have the same level of security awareness or training as IT professionals, which can increase the risk of human errors [8]. Furthermore, SCADA systems often involve multiple vendors and

protocols, which can increase the complexity of the systems and make it more difficult to secure them. Among the malware types, ransomware has been utilized in recent years to extort victims by locking their personal and operational data in exchange for a ransom [9]. There is no doubt that ransomware attacks are on the rise as well as some other types of cyberattacks. Therefore, the ways to properly address the problem are important.

Not only are PCs and mobile devices targeted by ransomware attacks, but also Industrial Internet of Things (IoT) and SCADA systems [10]. The issue is exacerbated in cyber-physical and industrial systems such as SCADA due to the adoption of security measures and procedures from the traditional systems [11]. These measures and procedures do not fully conform or fit with the SCADA environment and context due to their special nature and the data exchanged between each of the critical components. These aspects are highly dependent on the system context, operations, and data-processing flow. Such aspects can be investigated through several factors that contribute to deterring the momentum of ransomware attacks in industrial control systems (ICS).

1.1. Recent ICS Ransomware Attacks

There have been several recent ransomware attacks against ICS, including SCADA. In 2021, two major ransomware attacks targeted critical infrastructure in the United States [12]. In May, Colonial Pipeline, which supplies gasoline and jet fuel to much of the East Coast [12], was hit by a cyberattack that disrupted its operations for several days. The incident resulted in fuel shortages, panic buying, and price increases in multiple states. Then, in June, JBS, the world's largest meat supplier, was targeted by a similar attack that forced the company to shut down its plants in the US and Australia. The attackers used a variant of the Ryuk ransomware to encrypt the company's systems and demanded a ransom of several million dollars. These attacks caused significant financial losses for both companies, with Colonial Pipeline reportedly paying a ransom of $4.4 million to the attackers and JBS paying $11 million. In October 2021, a ransomware attack on the Czech Republic's largest power company, CEZ, resulted in the shutdown of several power plants and the disruption of the electricity supply to thousands of customers. The attackers used the Winnti malware to gain access to the company's systems and then deployed the RansomExx ransomware. In December 2020, the Cybersecurity and Infrastructure Security Agency (CISA) issued an emergency directive regarding a ransomware attack on a natural gas compression facility; the attackers used a variant of the TrickBot malware. These examples demonstrate that ransomware attacks on ICS can have serious consequences and can cause significant disruption to critical infrastructure. These incidents highlighted the need for increased cybersecurity measures and sparked discussions about the vulnerability of critical infrastructure to cyberattacks. The attacks also demonstrated the potential for significant economic and social disruptions as a result of these types of attacks. Therefore, it is important for organizations that operate industrial systems to take steps to protect their systems from these types of attacks, by implementing robust cybersecurity measures and regularly updating and patching their systems.

1.2. Objectives and Contributions

Numerous studies have been conducted proposing ransomware detection and mitigation solutions. Some of these studies tackled the problem in SCADA systems. However, there is a lack of investigative studies that addressed the problem. Therefore, the research community needs to establish a more comprehensive state-of-the-art knowledge base of the current risks related to the ransomware problem within the SCADA domain. Consequently, this paper is a comprehensive survey of the current solutions, open issues, and research directions. To the best of our knowledge, this is the first survey paper that explores the answers to reducing and/or preventing ransomware attacks targeting SCADA systems.

In this survey, we selected articles based on their relevance to predicting ransomware attacks. Due to the narrow focus of the survey, we limited the number of articles to those specifically addressing ransomware prediction. Therefore, we conducted a non-

systematic literature review to analyze the available literature. The contribution of this paper is threefold:

- We identify existing studies pertaining to ransomware attacks on SCADA systems and highlight the differences to establish our unique contribution;
- We discuss both technical and organizational aspects of the ransomware problem;
- We provide a generic situational-based framework that can be used to design solutions that combine the technical and environmental factors dealing with ransomware attacks on SCADA.

2. Related Works

The adoption of Internet-connected devices in industrial systems such as SCADA increased the likelihood of cyberattacks as well [11]. In recent years, several incidents involving malware attacks against ICS have been dissected and analyzed [13–15]. This is due to the advantage that those malicious programs give to the attacker which allows them to carry out automated, high-profile attacks with little effort. To mitigate these cybersecurity concerns, organizations need to implement robust security measures for SCADA systems, such as implementing secure remote access protocols, regularly updating and patching the systems, and providing security training for operators and maintenance personnel [16]. Additionally, organizations need to conduct regular security assessments and penetration testing to identify vulnerabilities and weaknesses in the systems [17].

2.1. SCADA Ransomware Surveys and Challenges

Ransomware is a popular research topic and several surveys have been conducted to study its various aspects. The survey conducted by [18] examines SCADA systems' architecture, vulnerabilities, and attack vectors due to TCP/IP network integration, and analyzes ransomware, its phases, and encryption techniques. It establishes a risk assessment for ransomware injection in SCADA systems, noting that budget constraints often result in inadequate isolation and therefore exposure to threats. The study highlights the potential damage caused by ransomware attacks on critical infrastructure and recommends prioritizing ransomware protection in risk management and incident response plans. However, the survey neither discussed the solutions proposed for preventing and predicting ransomware attacks nor highlighted the effect of the situation and context in which the attacks occur. Likewise, ref. [19] examined the security vulnerabilities of SCADA systems and categorized the threats. It reviewed SCADA systems' architecture, vulnerabilities, attacks, intrusion detection techniques, and testbeds as well as proposed an attack taxonomy based on specific criteria. Moreover, the survey discusses the general threats and does not discuss predicting the likelihood of a ransomware attack.

Another survey [20] provides an analysis of ransomware attacks pertaining to PCs/workstations, mobile devices, and IoT/CPS platforms. This survey covers studies completed from 1990–2020, which offers insights into ransomware evolution, key components, a taxonomy of significant ransomware families, and an extensive overview of countermeasures, including analysis, detection, and recovery across various platforms (i.e., not just SCADA). Similarly, [21] offered a survey on the evolution, prevention, and mitigation of ransomware in an IoT context, providing insights into IOT ransomware evolution. The authors strived to dissect the various aspects of attacks, including ransomware strains, current research, prevention, and mitigation techniques, handling affected machines, deciding on ransom payment, and future trends in IoT ransomware propagation. However, solutions related to the early prediction of ransomware were not discussed in either survey.

The investigators in [22] have noted recent progress in analyzing, detecting, and preventing ransomware attacks. They discuss ransomware detection and prevention methods, and the testing of ransomware samples, and have proposed a new experimental ransomware detection addon called AESthetic, which is incorporated into antivirus software for the purpose of preventing such attacks. Their survey analyzes the effectiveness of countermeasures and identifies several future research challenges. Another survey

by [23] compares and classifies recent ransomware detection techniques and their respective decision-making procedures to distinguish between benign and malicious strains. Both studies focused only on the detection and prevention of ransomware without discussing the early prediction of such attacks. Consequently, the need to better define this gap in terms of the existing literature discussing the likelihood of an attack given the contextual circumstances is needed. Our paper strives to investigate how situational awareness, including context, can be incorporated into those solutions as an additional layer.

2.2. Ransomware Attacks on SCADA

Ransomware targets a broad spectrum of sectors, including critical infrastructure such as transportation, telecom, logistics operations, public agencies, and healthcare [24]. Moreover, with the recent disruption of Colonial Pipeline's 100 million gallons of daily fuel supplies and the halting of JBS's beef-processing operations, ransomware attacks hit heavily on industrial sectors causing major losses to the victims and consumers.

By utilizing the cryptography-related application programming interfaces (APIs) embedded into the operating systems, ransomware can efficiently run in various environments with minimal memory and processing resources [25]. Different ransomware categories exhibit various behaviors related to encrypting data and locking services. Such encryption can be easily performed using the libraries and functions embedded in the underlying operating system [26]. Therefore, the distinction between ransomware-based encryption and innocent encryption is challenging as they both use the same libraries and APIs.

Based on the targeted resource and the attack mechanism, ransomware can be classified into two categories, namely, locking ransomware and crypto-ransomware [27]. While the former disables one or more key services provided by the targeted system, the latter encrypts the data and/or user-related files. Therefore, the key difference between ransomware and traditional malware is the use of a system's own component (like cryptographic routines or hardware) to attack another component (like the file system) [12]. This makes it easy for ransomware developers to create unbreakable, sophisticated programs with little effort, which explains the trend of ransomware attacks in recent years.

Unlike traditional malware and cyberattacks, thwarting ransomware needs to be more proactive due to the irreversible damage that it may inflict on the victim's data [28] and operations. While the malware effect could be reversed by simply removing the malicious software, the ransomware's encrypted data cannot be accessed without the help of the ransomware's owner [10]. Therefore, it is more feasible to be proactive and prevent the attack in the first place. As prevention needs the involvement of the system user (i.e., victim) to some extent, the human and managerial factors become of significant importance. However, such an aspect of cybersecurity governance that helps to protect against ransomware attacks is mostly overlooked by the research community.

The factors concerning the proliferation of ransomware attacks are discussed in several studies. The study conducted by [29] investigated several pre-existing constraints that lead to an increasing number of successful ransomware attacks. Among these factors is the difficulty of identifying bottlenecks in the system proactively. The diversity of components and stakeholders at all levels of the system is another factor as the awareness and preparedness vary and one weak component could have a cascading effect on the other components. According to this study, organizational and personality differences influence the efficacy of the policies and countermeasures pertaining to ransomware attack prevention. Qualitative semi-structured interviews with focused groups have been conducted by [30] to investigate ransomware attack strategies against different business environments. Several aspects have been explored including attack vectors, targeted victims, and the nature of the industry. The study shows that ransomware attacks target individual users and machines. It also shows that emails and brute-forcing are the commonly used infection vectors employed by the attackers to deliver the payload to the target.

2.3. Research Related to Ransomware Countermeasures

Ransomware countermeasures can be categorized into detection, prevention, and prediction. The detection approach utilizes the known attack patterns to build a model that can detect attacks with similar behavior. Ransomware detection provides a proactive measure on which the prevention takes place. Prevention is a specification approach that relies on predefined rules and procedures to stop attacks when it happens [31]. These roles and procedures are constructed manually based on human discretion. Hence, prevention is static and prone to error.

2.3.1. Ransomware Prevention

Typically, studies that focus on prevention identify the various factors and parameters that can influence the quality of the preventive measures [31]. The performance of prevention frameworks depends heavily on quality factors. Predictions can also be used as a proactive measure that improves prevention capabilities. Although several studies developed prediction models for malware attacks, they use historical data as the basis for prediction [32–35]. While this approach may be suitable for systems whose behavior is static, it cannot be applied for ransomware attacks as the behavior is dynamic due to obfuscation strategies such as polymorphism and metamorphism employed by attackers. In addition, the existing predictive models are built out of the context from overseeing the situation in which the ransomware attacks take place. In this section, a dozen or more studies related to ransomware prediction are identified and discussed.

The factors influencing ransomware threat avoidance were explored by [36]. This study exposed the interactions between several factors such as the subjective norm, the attitude towards knowledge sharing, the experience of threats, and how such interactions affect threat avoidance behavior. Moreover, this study identified the cascading effect of the interaction of factors that act as a chain of nodes whose one node influences the proceeding node and is influenced consequently by its preceding node, and so forth. The study focused on college students within the United States. An empirical study to assess the ransomware-related severity factors was conducted by [37]. The study investigated the effect of a set of factors on the degree of severity. Among the studied factors are the organization's size, security posture, propagation class (a.k.a. the degree of ransomware sophistication), and type of attack target. An impact assessment was carried out involving several items such as the business continuity disruption timeframe, recovery time, affected devices, and information loss.

A set of ransomware success factors were proposed by [38], including anonymous payment methods, the adoption of system-owned cryptographic libraries, and easy-to-use ransomware development kits. However, all previous studies approached the factors related to ransomware attacks in isolation from the targeted environment. That is, those factors were investigated in general without considering the operational environment. This makes the findings and proposed hypothesis difficult to reflect on a particular scenario or system. For SCADA systems, several ransomware attacks' key success factors have been investigated [11]. The study tried to focus on the factors related to the operational aspects of the system. Resource limitation and incompatibility between the SCADA system and security measures and security protocols were among the issues that were highlighted.

The study conducted by [39] investigated the interaction between the users, anti-virus software, and malware. An empirical experiment has been conducted to measure several factors that influence the spread of malware on victims' devices. The study concluded that the use of the Internet, peer-to-peer applications, and computer expertise are found to be more influential in the rise of malware attacks. The relationship between user activities and malware infections was also investigated by [40]. Routine activity theory was used to measure to what extent the convergence of motivated attackers and vulnerable targets could increase the likelihood of malware infections. The study concluded that the legitimate use of computers has a weak correlation with a malware infection. Such correlation becomes stronger when victims use illegitimate (pirated) software.

2.3.2. Ransomware Prediction and Detection

Organizational and managerial factors are not the only aspect that can be explored for situational-awareness-based protection against ransomware attacks but also the system's operational parameters. That is, the data collected from the running process of ransomware can be combined with the organizational and managerial data so the model can predict based on the behavior of both the ransomware and the system. This makes the model situationally aware of future attacks that consider not only the development of ransomware behavior but also the system's vulnerabilities. Therefore, the model can adapt to the operational and behavioral changes of the ransomware and target system.

Several studies were conducted to investigate the use of intelligent prediction engines to predict potential malware and ransomware attacks. In the study [41], they used the generative adversarial network (GAN) to predict future malware variants. The GAN was used to generate new malware samples based on existing ones. The data were generated by observing existing malware signatures and producing similar signatures. The signature is derived from the static analysis of malware payloads.

The MalDeepNet [42] is a model constructed to predict the behavior of malware and construct artificial patterns that represent the trend of malware behavior. The new patterns are then added to the existing malware dataset, which was used to train a cluster-based detection engine. Likewise, MalGAN [43] is a GAN-based malware generator that is used to develop malware black-box attacks. MalGAN utilizes a generator to create the malware samples and a substitute detector to train the black-box malware detection system. A generative network is trained to minimize the generated adversarial samples needed to produce the specific malicious probabilities that would be predicted by the substitute detector.

Another study by [44] conducted a behavioral analysis of the ransomware attack process and developed a model that predicts the future behavior of the malware. The study relies on data related to the attack process, file system, persistence, and network analysis. The model was built using supervised machine learning. The idea is to watch, learn, and predict how the malware will evolve toward achieving its goal with very little data. However, the study is limited to data that represent the previous attack behavior regardless of the context in which the attack has taken place. This adversely affects the model's accuracy when dealing with sophisticated and targeted attacks that change their behavior according to the context.

A logistic regression prediction model [45] was developed to circumvent the new malware attack. The model was trained using a dataset of previous malware infections. The model introspects the patterns in the data and analyzes the progression of the attack behavior. Likewise, the light gradient-boosting decision tree was used by [46] to predict future malware attacks on cloud systems. The model uses malware behavioral data to train the decision tree classifiers. Similarly, the study conducted by [47] developed a regression-based neural network model to forecast short-term ransomware behavior based on historical time-series data. These models only focus on data related to processing operations, but the context in which the process was running has been ignored.

A predictive model [48] for ransomware attacks on IoT devices was conducted using the context ontology for feature extraction [49]. The use of contextual data helps to reduce the computational complexity needed, which makes it suitable to run on resource constrained IoT devices. The context ontology focuses on a subset of known ransomware attack vectors based on the assumption that the targeted devices are of the IoT type. However, relying only on contextual data for lightweight modeling is not enough to capture the characteristics of the evasive malware as it drops the behavioral data which is imperative for predicting the future behavior of the malware.

The deep learning represented by long short-term memory (LSTM) was utilized by [50] to provide an early prediction of malware attacks in Android devices. The model helps to protect Android devices from malware attacks by the early prediction of suspicious behavior. It captures the implicit contextual relations between various data generated by

the running application. However, the model predicts the suspicious behavior of a running process based on the data captured in the early phases of the attack during the same session. Such an approach lacks the sufficient data needed for accurate prediction and is unable to predict the future behavior of the malware. Table 1 summarizes the studies related to ransomware prediction. It gives a brief description of the problems those studies have tried to address, with the solutions they proposed, methods, tools, and limitations.

Predictive modeling can help to mitigate and prevent future attacks by tracing the attack development over time. It can be developed using a combination of operational data and managerial data. The operational data are collected from the running process of the ransomware. The data consist of the process-tracing activities as well as the situational data representing the context surrounding the running environment. The situational data consolidate the operational data by adding context to the operational data. This is imperative for ransomware attack prediction as many of those malware applications can adaptively change their behavior according to the context. Furthermore, situational data can also be collected from many sources related to the system of interest using threat intelligence. Together with contextual data, situational data can enrich the knowledge base of the prediction model. Nonetheless, this type of data fusion was overlooked by existing studies.

Table 1 summarizes the studies related to ransomware behavior prediction. It can be concluded that current studies rely solely on operational data extracted from the running process of the ransomware on the system. These data contain information about the interaction between the malicious process and the resources in the target system and are used to train machine-learning models for detecting and predicting attacks. However, these studies rely on historical data that do not capture how ransomware behavior evolves over time, and they ignore environmental factors that affect the behavior of ransomware when running. As ransomware can change its behavior based on several factors, including the running environment, current security posture, and the situation on the targeted system, predictive models for ransomware attacks on SCADA must take these factors into account. Researchers and security professionals can address these limitations when designing predictive models for ransomware attacks.

Table 1. Studies related to ransomware behavior prediction.

Author	Problem	Solution	Method	Tools	Empirical	Limitation
[32]	Existing approaches to detect the malware need to collect enough data which takes more time, during which the sabotage has likely already been inflicted by the time of detection.	Predicting the behavior based on a short snapshot of behavioral data.	An ensemble RNN. The method was able to predict the attack within 5 s with an accuracy of around 94 %.	Keras, and Tensorflow	Yes	The method relies on historical data to predict the behavior. This approach is not suitable for obfuscated behavior that tries to show a major difference between past and future attacks.
[50]	Due to the obfuscation techniques employed by advanced malware, detection is no longer enough, and there is a need for methodologies to predict future behavior instead.	A rapid sequence snapshot analysis was used to make the prediction decisions.	A set of random snapshots were taken from the APIs and permission data and used to train an ensemble LSTM model that is used for the prediction.	Tensorflow	Yes	The LSTM was trained on historical data only, which assumes that these historical attack patterns are likely to reoccur in future attacks. This does not hold, especially with the use of obfuscation and polymorphic strategies adopted by the malware to change the attack behavior.
[33]	The detection of ransomware based on past attack data is not suitable to detect novel, zero-day attacks, which are common nowadays.	The behavioral patterns extracted from the dynamic analysis of ransomware during the execution time were used to train a prediction model.	Support vector machines (SVM) were used to build the prediction model based on the behavioral data.	Scikit Learn, and Pandas	Yes	This approach also uses historical behavior to predict future ones. This is not suitable for evasive ransomware that uses obfuscation and polymorphism to change its behavior from time to time.
[34]	Advanced malware can obfuscate much of its traces through many mechanisms, such as metamorphic engines. Therefore, the detection of such malware has become a significant challenge for malware analysis mechanisms.	A regression model to predict advanced malware based on a selected set of significant features extracted from a dataset of malware runtime data.	The dataset is created by executing real-world malware samples and capturing the behavioral data into trace files.	N/A	Yes	The model was trained using historical data of existing and known malware samples. The dataset does not contain the future behaviors necessary for accurate prediction models.
[35]	Sophisticated Android malware families often implement techniques aimed at avoiding detection. Split-personality malware, for example, behaves benignly when it detects that it is running on an analysis environment such as a malware sandbox, and maliciously when running on a real user's device.	Exploiting sandbox detecting heuristic prediction to predict and automatically generate bytecode patches.	An Andronew, a heuristic approach, was used based on API calls collected during the execution time of the malware.	Sandbox	Yes	The heuristics were performed based on historical data, which limits the ability of this approach to predict the future behavior of malware

Table 1. *Cont.*

Author	Problem	Solution	Method	Tools	Empirical	Limitation
[41]	Zero-day malware attacks are challenging due to the polymorphic nature of the malware.	Generating synthesized malware samples based on existing malware signatures derived from the static analysis of malware payloads.	GAN algorithm to generate artificial malware samples.	Keras, and Tensorflow	Yes	The static analysis adopted by the study does not reveal the behavioral aspect of the malware as polymorphism works during the runtime. In addition, the packing and encryption techniques used by sophisticated malware prevent the static analysis from exploring the malware features.
[42]	Existing malware detection is not accurate enough.	A cluster-based detection engine that is trained based on artificial patterns represents the trending of malware behavior.	GAN algorithm to create malware patterns.	N/A	N/A	There was no evidence of the applicability and efficacy of the model.
[43]	Malware authors have the ability to reveal the features used by detection models.	MalGAN model that attacks black-box machine-learning detection models.	A substitute detector to fit the black-box malware detection system.	N/A	Yes	The data used for model training were general and limited to malware operational behavior. The context was not captured.
[44]	The ransomware changes its behavior which makes it difficult to detect.	The study studies data collected from the ransomware process and its interaction with the file system.	It used malware development toolkits to create ransomware samples.	ADMMutate, Clet, and Phatbot	Yes	The study is limited to the ability of the tools to manually create samples, which makes it impractical to have a diversified dataset.
[45]	Detecting novel malware attacks is difficult as the behavior changes continuously.	The model examines the patterns in the data and studies the evolution of the malware behavior.	It used a collection of data from previous malware infections to train a logistic regression algorithm.	N/A	Yes	Relying on the evolution of the attack behavior to forecast future attacks is not sufficient to visualize the sophisticated malware attacks.
[47]	The new types of malware tend to be more difficult to detect than older ones. This has made content-based, signature-based, and pattern-matching techniques less effective in detecting and preventing ransomware attacks.	Utilized the neural network algorithm to predict the future occurrences of ransomware and malware attacks over time.	Time-series regression-based neural network algorithm model.	TensorFlow, Keras, NumPy, Matplotlib, and Pandas	Yes	The model concentrates solely on data pertaining to processing operations, disregarding the context in which the process was executed.

Table 1. *Cont.*

Author	Problem	Solution	Method	Tools	Empirical	Limitation
[48]	Existing ransomware attack predictions are not tailored for IoT systems that are diverse and resource-constrained environments.	A technique for predicting ransomware using contextual data and utilizing a context ontology to gather information characteristics of ransomware attacks against the IoT.	An ontology approach with SVM.	N/A	Yes	Relying only on contextual data and ignoring the behavioral data is insufficient for modeling the characteristics of the evasive malware attacks.
[50]	Detection solutions alone are no longer enough to protect against malware due to the increasing rate of zero-day attacks.	An early prediction of malware attacks in Android devices was proposed. By capturing the implicit contextual relations between various data, the model predicts the suspicious behavior of a running process using data collected during the early stages of the attack within the same session.	LSTM and ensemble learning.	N/A	Yes	This approach is inadequate in terms of the necessary data required for an accurate prediction and is unable to anticipate the future behavior of the malware.

3. The Data Used for Ransomware Behavioral Analysis

To study the behavior of ransomware attacks, researchers typically rely on data collected from various sources, including malware analysis reports, network traffic logs, and incident response reports [25]. These data can provide insight into the tactics, techniques, and procedures (TTPs) used by ransomware attackers, as well as the vulnerabilities they target and the types of data they seek to encrypt. One of the primary sources of data used in ransomware research is malware samples [27]. Security researchers can analyze these samples to identify the specific strain of ransomware and the methods used to encrypt files and demand payment. Researchers can also use sandboxing and emulation techniques to simulate the behavior of ransomware in a controlled environment, allowing them to study the malware's TTPs and identify potential mitigation strategies [24].

Sandboxing is a technique used to analyze the behavior of ransomware in a controlled environment. In a sandbox, the malware is isolated from the rest of the system and run in a virtual environment where its actions can be monitored and recorded [27]. By observing the malware's behavior in this way, security researchers can gain valuable in-sight into the tactics, techniques, and procedures (TTPs) used by ransomware attackers. Sandboxing allows researchers to identify the specific files and folders targeted by the ransomware, the encryption methods used, and any attempts to communicate with command and control (C2) servers [26]. This information can then be used to develop more effective detection and mitigation strategies. Sandboxing is a powerful tool in the fight against ransomware, allowing researchers to study the behavior of malware in a safe and controlled environment without risking the integrity of the system or the data it contains.

There are several well-known sandboxes that are commonly used for ransomware analysis, including:

- Cuckoo Sandbox: a popular open-source sandboxing platform that is widely used for malware analysis, including ransomware. It supports multiple operating systems, including Windows, Linux, and macOS, and allows researchers to monitor the behavior of malware in a virtual environment;
- Any.Run: a cloud-based sandboxing platform that allows users to analyze malware behavior in real-time. It supports a wide range of file types and provides detailed reports on the malware's behavior, including network connections, file modifications, and registry changes;
- Hybrid Analysis: a malware analysis platform that combines sandboxing with threat intelligence to provide a comprehensive view of malware behavior. It supports multiple file types, including executables, documents, and archives, and provides detailed reports on the malware's behavior and indicators of compromise (IOCs);
- VMRay Analyzer: a sandboxing platform that uses virtual machine introspection (VMI) to analyze malware behavior. It supports a wide range of file types and provides detailed reports on the malware's behavior, including network connections, file modifications, and memory analysis.

These sandboxes are just a few examples of the many tools and platforms available for ransomware analysis. Each has its own strengths and weaknesses, and researchers may choose to use multiple sandboxes to gain a more comprehensive view of malware behavior.

In addition to malware samples, network traffic logs can provide valuable data for studying ransomware attacks [24]. By monitoring network traffic during an attack, researchers can identify the patterns and indicators of compromise (IOCs) associated with ransomware, such as communication with command and control (C2) servers or attempts to access and encrypt specific files [28]. This data can be used to develop intrusion detection and prevention systems (IDPS) to alert organizations to potential ransomware attacks and block them before they can cause damage. The behavioral data collected during ransomware analysis can vary depending on the specific techniques and tools used, but some common types of behavioral data include:

- File system activity: information on which files and directories the ransomware accesses, modifies, or encrypts during an attack;
- Network activity: Data on the servers with which the ransomware communicates, the ports it uses, and the protocols it employs.;
- Registry modifications: changes made to the Windows registry by the ransomware, such as the creation or modification of registry keys;
- Process activity: information on the processes created or modified by the ransomware during an attack, as well as any child processes spawned by the malware;
- System configuration changes: changes made by the ransomware to system settings or configurations, such as changes to firewall rules or user account permissions;
- Memory analysis: the analysis of the ransomware's behavior in memory, such as code injection, process hollowing, or other memory-based attacks;
- Behavioral indicators: specific patterns or behaviors associated with ransomware attacks, such as attempts to disable security software, or the presence of specific file types or extensions commonly targeted by ransomware.

By analyzing these behavioral data, security researchers can gain insight into the techniques and tactics used by ransomware attackers, as well as identify potential vulnerabilities and mitigation strategies.

4. Research Direction and Future Work

In the previous discussion on limitations, we noted that existing solutions for defending against ransomware attacks tend to approach the problem from a single perspective focusing on operational or managerial aspects. This approach ignores the situational factors that accompany attacks and can make the proposed solutions unsuitable or ineffective. Therefore, there is a need to combine both approaches to develop security solutions that consider the specific situation and context surrounding each incident. In this way, solutions can be tailored to the systems they protect. To this end, we propose a generic framework in this section that future research can use to develop situational-aware solutions such as ransomware prediction: in other words, our view, namely, one that provides a situational awareness that can trigger an active response toward preventing the attack (prediction can be used to assess the strength of using different hardening strategies). By including situational awareness into the framework, the model would be able to predict potential attacks as soon as enough evidence is acquired from different sources. Therefore, this survey intends to give the framework as a direction for future research. It provides a baseline for our assessment of the various investigations to understand better how to compare their contribution and efficacy. The framework is a generic guideline that the research community can make use of when building more effective, situational-aware ransomware prediction solutions. The framework helps future research to be more proactive so the attacks can be prevented as early as possible which is necessary due to the irreversible nature of ransomware attacks.

4.1. Research Direction: Situational Awareness Ransomware Prediction Framework

To construct the framework, situation awareness is implemented through processes that vertically integrate organizational policy within managerial policy, which in turn is horizontally incorporated with the human factor. The key ingredients in the proposed framework are (1) the stakeholders (end users, cyber security team, and managerial team), (2) framework inputs (SCADA design, cyber security policy playbooks, threat intelligence, and operational data), and (3) framework outputs (perception, comprehension, and projection). Figure 1 illustrates the design of the proposed framework. To acquire data pertaining to situation awareness about ransomware attacks, it is necessary to (1) collect the incident-related data from the SCADA environment (perception), (2) synthesize elements of the ransomware incident with existing knowledge, and identify the severity of the incident with respect to cybersecurity objectives (comprehension), and (3) construct possible ransomware incident scenarios that might happen in the near future to prepare for the appropriate

response (projection). The design of the framework is composed of three phases as shown in Figure 1. The framework's design is a tri-phase artifact; each phase corresponds to one module in the situational awareness approach.

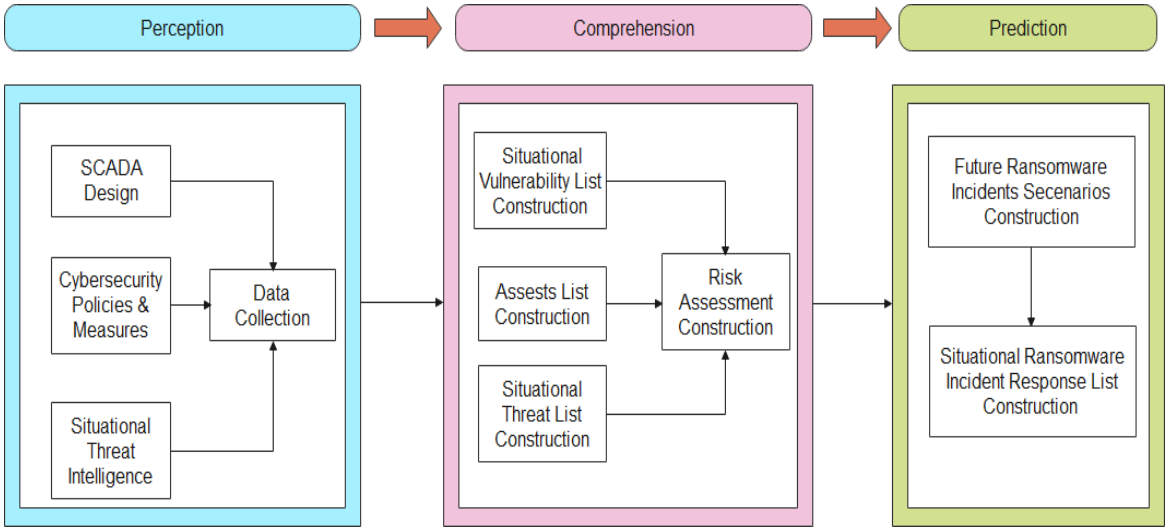

Figure 1. The proposed situational awareness ransomware incident response.

4.1.1. Perception Phase

The first phase is related to the perception module, in which data are collected from different sources. Three sources of data will be collected, namely, SCADA design, cybersecurity policies and measures, and situational threat intelligence. The data related to SCADA design and environment include but are not limited to nodes and devices interconnected with each other. It also includes the software and hardware specifications within the SCADA system. As part of this, the operational data are collected and/or exchanged between SCADA sensory nodes and other supervisory components. Ransomware attacks mainly deny access to these data by using the available cryptography mechanisms. Therefore, the information pertaining to collecting, storing, and processing these operational data is collected during the perception stage.

Cybersecurity policies and measures are the second sources of data collected during the perception phase of the situational awareness approach. It includes but is not limited to hardware/software security policies, data breach response policies, backup/recovery policies, and user identification, authentication, and authorization policies. Moreover, security measures currently in place are another source of data that will be collected during the perception phase. Additionally, situational threat intelligence data are collected based on the log files from different components in the SCADA system. The data collected from the three sources will be used as input for the next stage in the situation-awareness-based framework, i.e., comprehension.

4.1.2. Comprehension Phase

In the comprehension phase of the situation-awareness-based framework, the data acquired from the previous phase will be used to construct three lists, namely, the situational vulnerability list, asset list, and situational threat list. The combination of data will be introspected for constructing a risk tree and situational vulnerability assessment. The situational vulnerability list consists of a set of vulnerabilities in the SCADA system that ransomware could expose to break into and carry out the attack. The set of vulnerabilities is built based on the current situation and the setting applied to the SCADA system. This includes, but is not limited to, the current topology, operational conditions, workload, type of interaction, and amount of data. The vulnerability list is situational because it is derived based not only on the devices and assets that are potential targets but also on the current

operating conditions and number of resources in the SCADA allocated to support these operations. This list changes according to the change in the situation.

The asset list will be constructed based on the topology of the SCADA system. The assets include hardware, software, data, services, and applications. Communication channels and protocols are also considered assets. Additionally, items in the asset list will be paired with the priority of that asset. This priority will be used to measure the importance of the asset. Such importance will be determined based on the potential that this asset contributes to ransomware attacks. The proximity of an asset to the operational data is another factor to be considered when assessing the importance of the asset. Nevertheless, the importance of certain assets increases or decreases based on the situation. Adding a new device, sensor, and/or service could increase (or decrease) the importance of another asset. By adopting the situational awareness, items in the asset list will be reprioritized at any change in the SCADA system. Therefore, the importance of the items changes as such.

The third list that will be constructed during the comprehension phase is the situational threat list. In this list, the items are added and removed based on the degree of threat severity, and how much it contributes to successfully carrying out ransomware attacks. In such a manner, threats against data and devices where these data are stored and/or processed will have the highest priority. As a situational list, the items change based on the data-related factors such as the amount of data, processing capability, transmission efficiency, and real-time dependency. The three lists will be combined to construct the risk assessment that will be used as input for the projection, which is the third stage in the situational awareness framework.

To build the risk assessment, a threat tree will be constructed based on the vulnerability and asset lists. The threat tree takes as input the items in the asset list and the vulnerability list. The asset list will be categorized into three types, namely, hardware, software, and data. Likewise, items in the vulnerability list will be put under three categories: confidentiality, integrity, and availability. Each vulnerability category will then be used as the root of the threat tree. From each root, three branches will emit, each of which will be related to one category of the assets, i.e., hardware, software, and data. Each asset category will then be branched into several branches corresponding to the number of assets under that category. The leaves of the tree represent the set of threats to that asset. Each leaf in the threat tree will be assessed with two values: vulnerability level, and threat level. These values are estimated based on two factors: the relevance to operational data and the current situation within the SCADA system. The vulnerability level measures how vulnerable an asset is, whereas the threat level measures the degree of the threat on that particular asset. The threat tree will then be used to construct the risk assessment matrix where the rows represent the list of assets and the columns represent the type of vulnerability. The intersection of the row and column represents a risk value on a specific asset. This value will be calculated according to Equation (1) as follows:

$$\text{Risk} = \text{probability of attack} \times \text{consequence of attack} \quad (1)$$

The probability of attack and consequence of attack are estimated based on the threat–vulnerability values in the threat tree and asset priority (importance) in the asset list.

4.1.3. Projection Phase

Projection is the third phase of the situational awareness framework, in which the risk assessment constructed during the comprehension will be used to predict ransomware attacks on the SCADA system. The outcome of the situational risk assessment will be used to create several scenarios for ransomware attacks. When the situation changes, current scenarios are updated, or new scenarios are added. The purpose of creating these scenarios is to get the SCADA system ready for potential ransomware attacks in light of the current operational situation. For each scenario, a ransomware incident response will be prepared. According to the situation, the incident responses are updated and adapted when the list of scenarios is updated.

The projection is essential for preventing potential future ransomware attacks. Typically, such projection is made based on data gathered from various sources. Therefore, the data should represent the operational environment in which ransomware is executed. This includes the runtime data gathered during the execution of the ransomware running process and the situational data that reflect the operational environment of the process. By coupling both data types, the projection will be situational-aware, and does not only rely on the ransomware behavior but also the system parameters.

4.2. Suggestions for Future Works

Based on the literature reviewed, it is likely that the rise of ransomware targeting SCADA ICS will continue. This is due to the characteristics of SCADA systems that permit remote access and the interaction with diverse components, unique within bespoken environments, making them vulnerable to ransomware attacks. Ransomware can encrypt the operational data and disrupt the SCADA system, but predicting its behavior can aid in the development of proactive measures that enhance ICS security. However, current research efforts either concentrate on the operational side of attacks or the managerial and human aspects, neglecting the context in which the attacks occur. Previous investigations have also overlooked the evolutionary nature that allows ransomware to evolve its attacks with no or less similarity to existing attacks to negatively affect the defense systems to predict upcoming threats. Hence, the defense systems become less protective. This weakness negatively impacts the effectiveness of predictive modeling, as ransomware's behavior varies depending on the situation and context. As a result, there is a need to combine both operational and human factors when evaluating the probability of ransomware attacks. This can be accomplished by gathering data from the running malware process, the underlying operating environment, situational data related to organizational and human factors, and the system's current security posture, through a daunting set of tasks.

As deep learning has emerged as a promising technique for predicting ransomware attacks, it can be used to develop deep neural networks that can analyze vast amounts of data from various sources and identify patterns that indicate the likelihood of a ransomware attack. One direction of research is to develop multi-modal deep-learning models that consider multiple data sources, such as network traffic, system logs, and user behavior, to make more accurate predictions. Different modalities, such as network traffic data, system logs, and user behavior, can be used to build a more comprehensive representation of the system state and identify patterns that indicate the likelihood of a ransomware attack.

Another direction is to incorporate adversarial examples and defend against malicious attacks in the training process, to increase the robustness of the deep-learning models against real-world threats. Adversarial examples are intentionally crafted inputs that are designed to fool machine-learning models. Research in this direction aims to develop deep-learning models that can defend against such malicious attacks and improve the robustness of the models against real-world threats. Normally, generative adversarial networks (GAN) are used to generate artificial ransomware examples that represent the future behavior of the attacks.

Improving the interpretability of the deep-learning models is another research direction so that organizations can understand the reasoning behind the predictions and make informed decisions. The interpretability of deep-learning models refers to the ability to understand the reasoning behind the predictions made by the model. Research in this area aims to improve the interpretability of deep-learning models so that organizations can understand the factors that contribute to the prediction of a ransomware attack and make informed decisions.

In addition, research can also focus on developing transfer-learning models that can be trained on one domain and then transferred to another domain to improve the accuracy of predictions in new scenarios [51,52]. Transfer learning is a machine-learning technique where a model trained on one domain is applied to another domain. In the context of ransomware attack prediction, transfer-learning models can be trained on one

set of data and then transferred to another domain to improve the accuracy of predictions in new scenarios. This allows the predictive model to make use of data from similar (or generic) scenarios and applies it in a specific SCADA scenario. Transfer learning also helps to compensate data insufficiency by utilizing cross-domain knowledge. These research directions aim to address various challenges in the field of ransomware attack prediction using deep learning and also have the potential to significantly advance our understanding of ransomware attack profiles and their strategies, consequently improving the security of ICS against such threats.

5. Conclusions

This paper was developed to identify and explore the existing literature related to ransomware attacks within the general ICS context. This survey provides an overview of the current state of the art in ransomware attack prediction and highlights the potential of deep learning to advance the field. As the prediction of ransomware attacks is a critical area of research, this survey explored the state of the art and studies the related proposals. In this survey, we have focused on predictive modeling as well as the organizational and human factors influencing the performance of ransomware behavior prediction. A situational awareness framework for ransomware prediction that combines the behavioral and operational aspects of malware attacks was proposed as well. We also discussed the challenges and limitations of each approach and identified future research directions, such as the development of multi-modal deep-learning models, defense against adversarial attacks, improvement of model interpretability, and transfer-learning models. Further research is needed to address the challenges and limitations identified and to continue to improve the accuracy and robustness of ransomware attack prediction models.

Author Contributions: All authors have contributed equally in the manuscript. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Najran University, and the authors would like to thank them for their support.

Data Availability Statement: Not applicable.

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

References

1. Smadi, A.A.; Allehyani, M.F.; Johnson, B.K.; Lei, H. Power Quality Improvement Utilizing PV-UPQC Based on PI-SRF and PAC Controllers. In Proceedings of the 2022 IEEE Power & Energy Society General Meeting (PESGM), Denver, CO, USA, 17–21 July 2022.
2. Camargo, O.A.M.; Duarte, J.C.; Dos Santos, A.F.P.; Borges, C.A. A Review of Testbeds on SCADA Systems with Malware Analysis. *Rev. Inf. Teórica E Apl.* **2022**, *29*, 84–94. [CrossRef]
3. Aboaoja, F.A.; Zainal, A.; Ghaleb, F.A.; Al-Rimy, B.A.S.; Eisa, T.A.E.; Elnour, A.A.H. Malware detection issues, challenges, and future directions: A survey. *Appl. Sci.* **2022**, *12*, 8482. [CrossRef]
4. Abu Al-Haija, Q.; Smadi, A.A.; Allehyani, M.F. Meticulously intelligent identification system for smart grid network stability to optimize risk management. *Energies* **2021**, *14*, 6935. [CrossRef]
5. Fovino, I.N.; Carcano, A.; Masera, M.; Trombetta, A. An experimental investigation of malware attacks on SCADA systems. *Int. J. Crit. Infrastruct. Prot.* **2009**, *2*, 139–145. [CrossRef]
6. Nazir, S.; Patel, S.; Patel, D. Assessing and augmenting SCADA cyber security: A survey of techniques. *Comput. Secur.* **2017**, *70*, 436–454. [CrossRef]
7. Mir, A.W.; Kumar, K.R. An Enhanced Implementation of Security Management System (SSMS) using UEBA in Smart Grid based SCADA Systems. In *Applications of Machine Intelligence in Engineering*; CRC Press: Boca Raton, FL, USA, 2022; pp. 1–11.
8. Gómez, L.P.; Maimó, L.F.; Celdrán, A.H.; Clemente, F.J.G. Malware Detection in Industrial Scenarios Using Machine Learning and Deep Learning Techniques. *Adv. Malware Data Driven Netw. Secur.* **2022**, 74–93.
9. Reshmi, T. Information security breaches due to ransomware attacks-a systematic literature review. *Int. J. Inf. Manag. Data Insights* **2021**, *1*, 100013. [CrossRef]
10. Al-rimy, B.A.S.; Maarof, M.A.; Shaid, S.Z.M. Crypto-ransomware early detection model using novel incremental bagging with enhanced semi-random subspace selection. *Future Gener. Comput. Syst.* **2019**, *101*, 476–491. [CrossRef]

11. Gazzan, M.; Alqahtani, A.; Sheldon, F.T. Key Factors Influencing the Rise of Current Ransomware Attacks on Industrial Control Systems. In Proceedings of the 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 27–30 January 2021.
12. Alqahtani, A.; Sheldon, F.T. A survey of crypto ransomware attack detection methodologies: An evolving outlook. *Sensors* **2022**, *22*, 1837. [CrossRef] [PubMed]
13. Smadi, A.; Ajao, B.; Johnson, B.; Lei, H.; Chakhchoukh, Y.; Abu Al-Haija, Q. A Comprehensive survey on cyber-physical smart grid testbed architectures: Requirements and challenges. *Electronics* **2021**, *10*, 1043. [CrossRef]
14. Alghofaili, Y.; Albattah, A.; Alrajeh, N.; Rassam, M.A.; Al-Rimy, B.A.S. Secure cloud infrastructure: A survey on issues, current solutions, and open challenges. *Appl. Sci.* **2021**, *11*, 9005. [CrossRef]
15. Aboaoja, F.A.; Zainal, A.; Ghaleb, F.A.; Saleh Al-rimy, B.A. Toward an Ensemble Behavioral-Based Early Evasive Malware Detection Framework. In Proceedings of the 2021 International Conference on Data Science and Its Applications (ICoDSA), Bandung, Indonesia, 6–7 October 2021.
16. Butt, U.J.; Abbod, M.; Lors, A.; Jahankhani, H.; Jamal, A.; Kumar, A. Ransomware Threat and Its Impact on SCADA. In Proceedings of the 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3), London, UK, 16–18 January 2019.
17. Basnet, M.; Poudyal, S.; Ali, M.H.; Dasgupta, D. Ransomware detection using deep learning in the SCADA system of electric vehicle charging station. In Proceedings of the 2021 IEEE PES Innovative Smart Grid Technologies Conference-Latin America (ISGT Latin America), Lima, Peru, 15–17 September 2021.
18. Ibarra, J.; Butt, U.J.; Do, A.; Jahankhani, H.; Jamal, A. Ransomware impact to SCADA systems and its scope to critical infrastructure. In Proceedings of the 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3), London, UK, 16–18 January 2019; pp. 1–12.
19. Alanazi, M.; Mahmood, A.; Chowdhury, M.J.M. SCADA Vulnerabilities and Attacks: A Review of the State-of-the-Art and Open Issues. *Comput. Secur.* **2022**, *125*, 103028. [CrossRef]
20. Oz, H.; Aris, A.; Levi, A.; Uluagac, A.S. A survey on ransomware: Evolution, taxonomy, and defense solutions. *ACM Comput. Surv. CSUR* **2022**, *54*, 1–37. [CrossRef]
21. Humayun, M.; Jhanjhi, N.Z.; Alsayat, A.; Ponnusamy, V. Internet of things and ransomware: Evolution, mitigation and prevention. *Egypt. Inform. J.* **2021**, *22*, 105–117. [CrossRef]
22. Beaman, C.; Barkworth, A.; Akande, T.D.; Hakak, S.; Khan, M.K. Ransomware: Recent advances, analysis, challenges and future research directions. *Comput. Secur.* **2021**, *111*, 102490. [CrossRef]
23. Berrueta, E.; Morato, D.; Magaña, E.; Izal, M. A survey on detection techniques for cryptographic ransomware. *IEEE Access* **2019**, *7*, 144925–144944. [CrossRef]
24. Urooj, U.; Maarof, M.A.B.; Al-rimy, B.A.S. A Proposed Adaptive Pre-Encryption Crypto-Ransomware Early Detection Model. In Proceedings of the 2021 3rd International Cyber Resilience Conference (CRC), Langkawi Island, Malaysia, 29–31 January 2021.
25. Olaimat, M.N.; Maarof, M.A.; Al-rimy, B.A.S. Ransomware Anti-Analysis and Evasion Techniques: A Survey and Research Directions. In Proceedings of the 2021 3rd International Cyber Resilience Conference (CRC), Langkawi Island, Malaysia, 29–31 January 2021; IEEE: New York, NY, USA.
26. Ahmed, Y.A.; Huda, S.; Al-Rimy, B.A.S.; Alharbi, N.; Saeed, F.; Ghaleb, F.A.; Ali, I.M. A weighted minimum redundancy maximum relevance technique for ransomware early detection in industrial IoT. *Sustainability* **2022**, *14*, 1231. [CrossRef]
27. Ahmed, Y.A.; Koçer, B.; Huda, S.; Al-Rimy, B.A.S.; Hassan, M.M. A system call refinement-based enhanced Minimum Redundancy Maximum Relevance method for ransomware early detection. *J. Netw. Comput. Appl.* **2020**, *167*, 102753. [CrossRef]
28. Ahmed, Y.A.; Kocer, B.; Al-rimy, B.A.S. Automated analysis approach for the detection of high survivable ransomware. *KSII Trans. Internet Inf. Syst. TIIS* **2020**, *14*, 2236–2257.
29. Mierzwa, S.J.; Drylie, J.J.; Ho, C.; Bogdan, D.; Watson, K. Ransomware Incident Preparations with Ethical Considerations and Command System Framework Proposal. *J. Leadersh. Account. Ethics* **2022**, *19*.
30. Connolly, L.Y.; Wall, D.S. The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures. *Comput. Secur.* **2019**, *87*, 101568. [CrossRef]
31. Brewer, R. Ransomware attacks: Detection, prevention and cure. *Netw. Secur.* **2016**, *2016*, 5–9. [CrossRef]
32. Rhode, M.; Burnap, P.; Jones, K. Early-stage malware prediction using recurrent neural networks. *Comput. Secur.* **2018**, *77*, 578–594. [CrossRef]
33. Adamu, U.; Awan, I. Ransomware Prediction Using Supervised Learning Algorithms. In Proceedings of the 2019 7th International Conference on Future Internet of Things and Cloud (FiCloud), Istanbul, Turkey, 26–28 August 2019.
34. Bahtiyar, Ş.; Yaman, M.B.; Altınığne, C.Y. A multi-dimensional machine learning approach to predict advanced malware. *Comput. Netw.* **2019**, *160*, 118–129. [CrossRef]
35. Leguesse, Y.; Vella, M.; Ellul, J. *AndroNeo: Hardening Android Malware Sandboxes by Predicting Evasion Heuristics*; Springer International Publishing: Berlin/Heidelberg, Germany, 2018.
36. Acosta-Maestre, H.A. *The Empirical Study of the Factors that Influence Threat Avoidance Behaviour in Ransomware Security Incidents*; Nova Southeastern University: Ann Arbor, MI, USA, 2021; p. 95.
37. Connolly, L.Y.; Wall, D.S.; Lang, M.; Oddson, B. An empirical study of ransomware attacks on organizations: An assessment of severity and salient factors affecting vulnerability. *J. Cybersecur.* **2020**, *6*, tyaa023. [CrossRef]

38. Al-rimy, B.A.S.; Maarof, M.A.; Shaid, S.Z.M. Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. *Comput. Secur.* **2018**, *74*, 144–166. [CrossRef]
39. Lévesque, F.L.; Chiasson, S.; Somayaji, A.; Fernandez, J.M. Technological and human factors of malware attacks: A computer security clinical trial approach. *ACM Trans. Priv. Secur. TOPS* **2018**, *21*, 1–30. [CrossRef]
40. Holt, T.J.; Bossler, A.M. Examining the Relationship Between Routine Activities and Malware Infection Indicators. *J. Contemp. Crim. Justice* **2013**, *29*, 420–436. [CrossRef]
41. Moti, Z.; Hashemi, S.; Namavar, A. Discovering Future Malware Variants by Generating New Malware Samples Using Generative Adversarial Network. In Proceedings of the 2019 9th International Conference on Computer and Knowledge Engineering (ICCKE), Mashhad, Iran, 24–25 October 2019.
42. Lu, S.; Ying, L.; Lin, W.; Wang, Y. New era of deeplearning-based malware intrusion detection: The malware detection and prediction based on deep learning. *arXiv* **2019**, arXiv:1907.08356.
43. Hu, W.; Tan, Y. Generating adversarial malware examples for black-box attacks based on GAN. *arXiv* **2017**, arXiv:1702.05983.
44. Popli, N.K.; Girdhar, A. Behavioural Analysis of Recent Ransomwares and Prediction of Future Attacks by polymorphic and Metamorphic Ransomware. In *Computational Intelligence: Theories, Applications and Future Directions-Volume II*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 65–80.
45. Yeboah-Ofori, A.; Boachie, C. Malware Attack Predictive Analytics in a Cyber Supply Chain Context Using Machine Learning. In Proceedings of the 2019 International Conference on Cyber Security and Internet of Things (ICSIoT), Accra, Ghana, 29–31 May 2019.
46. Patel, V.; Choe, S.; Halabi, T. Predicting Future Malware Attacks on Cloud Systems using Machine Learning. In Proceedings of the 2020 IEEE 6th International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing, (HPSC) and IEEE International Conference on Intelligent Data and Security (IDS), Baltimore, MD, USA, 25–27 May 2020.
47. Albulayhi, K.; Al-Haija, Q.A. Early-Stage Malware and Ransomware Forecasting in the Short-Term Future Using Regression-based Neural Network Technique. In Proceedings of the 2022 14th International Conference on Computational Intelligence and Communication Networks (CICN), Al-Khobar, Saudi Arabia, 4–6 December 2022.
48. Mathane, V.; Lakshmi, P. Predictive analysis of ransomware attacks using context-aware AI in IoT systems. *Int. J. Adv. Comput. Sci. Appl.* **2021**, *12*, 240–244. [CrossRef]
49. Sadighian, S.A.; Robert, J.-M.; Sarencheh, S.; Basu, S. A Context-Aware Malware Detection Based on Low- Level Hardware Indicators as a Last Line of Defense. In Proceedings of the SECURWARE 2017: The Eleventh International Conference on Emerging Security Information, Systems and Technologies, Rome, Italy, 10–14 September 2017; pp. 10–19.
50. Amer, E.; El-Sappagh, S. Robust deep learning early alarm prediction model based on the behavioral smell for android malware. *Comput. Secur.* **2022**, *116*, 102670. [CrossRef]
51. Khan, M.; Naeem, M.R.; Al-Ammar, E.A.; Ko, W.; Vettikalladi, H.; Ahmad, I. Power forecasting of regional wind farms via variational auto-encoder and deep hybrid transfer learning. *Electronics* **2022**, *11*, 206. [CrossRef]
52. Mehedi, S.T.; Anwar, A.; Rahman, Z.; Ahmed, K.; Islam, R. Dependable intrusion detection system for IoT: A deep transfer learning based approach. *IEEE Trans. Ind. Inform.* **2022**, *19*, 1006–1017. [CrossRef]