Abstract — Wireless sensor networks have revolutionized the way healthcare works replacing the traditional methods with sensor-enabled IoT devices that help in monitoring the data. The data is collected by these sensors that are there on the body of the user, the data is transmitted over the network to the healthcare monitoring systems. The transmission follows the route of the wireless channel that is not secure as it can be accessed by legitimate as well as illegitimate users. These pose security threats; one such attack is a replication attack. This makes the replicas of the original node, replaces the data with the malicious content for attacking the system, and deploys the node back to the network making it difficult to detect. The aim of the work is to review the Blockchain-based intelligent monitored security system for the detection of replication attacks in the wireless healthcare network. The method used for review is the secondary research method. The main focus of the work is kept on the literature review for obtaining insights and knowledge. The results show that blockchain provides the required security to the data carried by the sensor-enabled IoT. The result contributed to the understanding of the different blockchain techniques in securing data. The system component is farmed in the work and verified in the results.

Keywords — blockchain, data analysis, distributed systems, healthcare system, predictive analysis, replication attack, secure data sharing, smart grid, traceability.

I. INTRODUCTION

Wireless healthcare networks have revolutionized the way the healthcare sector is monitored replacing the traditional method for efficiently operating the patient’s health [1]. As every technology comes with certain drawbacks along with benefits, the open-access nature of the network makes it vulnerable [2]. The unauthorized access behavior and open-end threats can pose security concerns to the patient's healthcare data. The data collected by the wearable devices for healthcare monitoring have security issues. One of the most challenging attacks is the replication attack [3]. This attack is on the sensor node carrying the sensitive healthcare data of the patient, the attacks replace the sensor nodes with replicas of the sensor nodes and replace the original data with fake data and deploys the sensor node back in the database [4].

Wireless healthcare systems are approachable to all the people around the globe, and this has reached every corner of the world [5]. The open-access nature of the technology of wireless healthcare networks and its wireless channels makes the transmission through the network unsecured [6]. The main aim of the work is to review the blockchain-based intelligent monitored security system for the detection of replication attacks in the wireless healthcare network. Blockchain is one of the most promising technologies for providing security [7]. Blockchain is known to provide a double layer of authentication and security to the data using cryptographic techniques and tools [8]. The data of the healthcare monitoring systems is observed and thus, detects such attacks on the wireless network of the healthcare monitoring system [8].

The work is structured as follows: Section II is a literature review that provides the overall understanding of the topic. The main focus of the work is centric on the review. The literature review explains the field of research, and the review is structured in different heading to provide the complete coverage of the topic. The system component table is included following the review. This states the common instances with the help of components and attributes for an overall view of the work. Section III explains the methodologies used for the work. Section IV; classification table, is also included. Section V is evaluation table. Section VI is system architecture. Section VII is the results and key findings of the work. Furthermore, Section VIII is discussion and Section IX is the conclusion that includes the major finding.

II. LITERATURE REVIEW

A. Field of Research

The research is made in the area of blockchain technology. The technology blockchain is evolving day by day with newer advancements. Blockchain technology provides security to the data using the cryptographic hash functions. The review is classified under different literature review headings. These explain the process from start to end and establish the knowledge in a hierarchical structure. The focus is made on

Chetanpal Singh, Charles Sturt University, Melbourne VIC 3000, Australia.
(e-mail: csingh@studygroup.com)
Prem Thapa, Charles Sturt University, Melbourne VIC 3000, Australia.
blockchain technology in eliminating the replication attacks for securing healthcare data. Different models and techniques are discussed for this in the review. The research gap is stated at the end of the review and different instances and attributes along with factors are placed in the component table.

B. Review

1) Wireless healthcare network and its security concerns

The Internet of Things (IoT) has advanced over time. IoT is considered to be the most prominent platform as it is dynamically used in resource sharing and helps in interconnecting different systems altogether. Reference [9] shows that one of the technical advancements of IoT can be seen in wireless healthcare networks. The platform connects different sensor nodes that monitors a patient’s health and transfer the data through the network to the healthcare systems. The authors state that wireless healthcare has benefited many across the globe, however; the open nature of wireless channels makes them vulnerable to security threats. These threats are targeted at the sensitive data of the patient [10]. This makes the users question the integrity of the technology. The attackers can misuse the data or sell it further to a third party. As this data is sensitive, this needs to be protected [11].

The advancement of wireless healthcare data has uplifted and upgraded the traditional way of healthcare monitoring. Reference [17] shows that, after the COVID 19 outbreak in recent years, this technique is used all around the world to fight against the pandemic. The authors explain that wireless healthcare monitoring systems are facing security issues. The threat of data confidentiality is surfacing as the data is facing a privacy leak [18]. This becomes one of the major challenges that the wireless healthcare system is facing. Attacks like DDoS, network conjunction, and many more overload the server with unwanted data to access the legitimate data [54]. This needs to be solved in order to get the proper aid to every person.

2) Threats associated with replication attack on WHN

There are many attacks that interrupt the secure data flow in the transmission of the data through the sensors of the wireless Healthcare Network (WHN). Reference [15] shows that out of many attacks of replication attack, the attacks on the CT scan and image processing is one of the major ones. These attacks block the server and manipulate the image processing systems. As stated by the author this makes it hard for the system to process. These attacks hamper the process of the healthcare monitoring systems and data carried by the system for processing [14]. These attacks need to be addressed to properly and securely proceed with the analysis of the data [13].

A replication attack is the kind of attack that replaces the original node with the fake node carrying the data that can attack the database and manipulates the entire database. Reference [18] shows that one of the most prominent attacks is the replication attack. It is hard to detect the source, as the node carries the same identity as the original one and pose as the legitimate one. It is further stated by the authors, that the node is efficiently deployed back in the data after changing the original data with the fake data [17]. The node carrying the personal and sensitive data of the user is exposed to multiple threats due to the open-access nature of the wireless channels [13].

3) Blockchain-based intelligent monitored security system

The outbreak of the pandemic of COIVD-19 has affected the medical services industry differently. The spread of COIVD-19 has been disturbing to the worldwide medical services industry, as this is one of its sorts of pandemics that are seen by the world to date. Reference [63] shows that this caused medical services to understand the issue with the keeping up of the information and maintaining it. As the quantity of patients is expanding step by step till today, the issue that the medical care industry is facing is the upkeep security of the information [14]. Blockchain is one of the emerging technologies that have the potential of maintaining security in the database [19]. Blockchain is known for providing the desired security layer with the implementation of cryptography along with securing the data [19].

Digital data is targeted with many attacks. Reference [20] shows that the data scavenging attack in the resource for monitoring carrying data faces data leak issues because of the attack. As the system needs security, the authors explain that the issues while sending the data and receiving can be solved using blockchain technology. Blockchain technology is proposed to overcome the security challenges in order to secure the data and its privacy [21]. Blockchain is known to be providing a dual layer of authenticity to the system using the cryptographic hash functions [22], [23]. Blockchain works on the principle of encrypting and decrypting for providing security to the system [24], [15].

4) Blockchain technology in replication attack detection

The pandemic recently has shaken the entire world. The outbreak of COVID-19 has alarmed the healthcare monitoring systems around the globe. Reference [25] shows that the pandemic has made every country revisit its healthcare monitoring infrastructure. The authors explain the healthcare system needs to keep a close tab on the patients suffering from the same. The vulnerabilities in the system make it a taking point. The databases lack in providing security to the system and ultimately the unauthorized can access the data [20]. Blockchain technology has made it easier for the monitoring system in providing security to the healthcare system [12], [19]. Blockchain is among the technology that eliminates the risks associated with unauthorized access [5]. Blockchain can easily detect attacks using the encryption technique. Blockchain provides security from end to end [12], [10].

The advancement of the IoT has made the healthcare monitoring system easier as compared to the traditional methods. The data is collected using the sensor-enabled IoT and transmits data through wireless channels. Reference [21] shows that the open-access behavior of the wireless sensor networks has made the system vulnerable to attacks. A replication attack is one of the kinds of attacks that target the node carrying the data [29], [18]. The node carrying the data is replaced with the
malicious node that is replicated and poses the same as the original node. The node is deployed back in the message and poses the same as the original. The author stated that the issue can be solved using the blockchain-based privacy-preserving scheme. This scheme realized the secure sharing of the medical data among the entities using the zero-knowledge proof. Blockchain provides dual security to the data for security [3], [26].

The revolution of the internet of things has helped to transform any object into network data with the help of WSN [2], [27]. This has provided the platform for many applications such as smart grids, smart homes, and smart cities [25], [28]. One of the major implementations of IoT is in healthcare monitoring. Reference [17] explains that these sensor-enabled pose certain threats in privacy leakage during the handling process of data. These issues have been addressed using the M-PPKS. This approach is based on homomorphic encryption that ensures that the privacy of the user is maintained and there is no leakage of data. This enhances mutual privacy in the healthcare system. Blockchain technology uses encryption and decryption techniques to ensure the security of the data in the database [29]-[31]. The security of the system is a must as it carries sensitive data relating to the patient [32], [34].

5) Secured wireless healthcare networks using blockchain technology

Blockchain has gained attention all around the world because of its characteristics of undeniable nature and the benefits and security it provides to the database. [35] explain that the limitations faced by the internet of things can be solved using blockchain technologies. Blockchain has the ability to provide security to wearable devices in healthcare systems. Blockchain has a higher bandwidth overhead, higher computation complexities, latency, and restricted scalability, these factors can’t be directly inherited in IoT [34], [36]. The authors discussed the ELIB model that is specifically made to fulfill the requirements of the IoT constrained. The blockchain ensures the complete security of the database and provides security to the data [37], [34].

The advent of blockchain technology has been revolutionary in recent years. Blockchain technology provides a secure platform for data. Blockchain enables data protection and detects anomalies in the system. Reference [35] explains that blockchain implementation secures healthcare services in the prediction of diseases in fog computing. Cardiovascular and diabetics are the disease that can be predicted by monitoring the health records collected with the help of healthcare wearables [66], [52]. The patient’s data is collected using the fog nodes and stored in a blockchain database. The clustering techniques are applied to the data collected. The data is sent further for the healthcare monitoring system to consider the data and act upon it. Blockchain provides a dual layer of security to the database [40], [47]. Implementation of blockchain in healthcare systems is very helpful [33], [46].

The modernizations of the healthcare sector have provided room for the implementation of the internet of things and applications based on healthcare systems [45], [23]. Reference [47] shows that the modification of healthcare monitoring has provided the users’ various benefits. The sensor-enabled devices help in monitoring the patient’s health. The data is collected by the wearables and transmitted to the healthcare system. The wireless channels used for the transmission of the data pose security threats in the data; this can be solved using blockchain technology [45], [8], [26]. Blockchain technology uses a cryptographic hash function in providing the necessary security to the data [43], [14]. The blockchain implementations have bought significant impacts in providing security, enabling encryption techniques [1], [47].

C. Research Gap

The authors explained the implementation of the blockchain-based intelligent monitoring system for securing the wireless healthcare network from replication attacks. Many authors have explored the aspects of replication attacks on healthcare systems and the effective use of blockchain in providing security to the database. However, the authors didn’t discuss the problems associated with the implementation of blockchain in the healthcare system. Blockchain implementation requires higher computational resources and is not that cost-effective.

D. System Component

Components of the system in general terms are described as the fundamental factors that are used to describe the overall process of the system. This work aimed to review blockchain-based intelligent systems for the detection of replication attacks in wireless healthcare networks. To get the insights and understanding of the work, 12 articles were selected that were reviewed in the work. The common components are selected in the work.

The component tables discuss the common instances based on the attributes from the selected 12 papers. The same is discussed in Table 1. The system component table is based on the simple steps of input-process-output-evaluation. The factors, attributes, and instances are selected from the selected research articles after deep analysis of the research articles. The factors such as healthcare data, blockchain-based monitoring, attack detection, and attacks are the process steps that are input, process, output, and evaluation. The attributes such as healthcare dataset, data capturing devices, the framework used, techniques, and more. The instances are searched in the selected articles and then filled in the table to provide overall understanding.

III. METHODOLOGIES

The methodologies are the process that is defined before the beginning of the work. The methodology is a process of defining the process, belief, and rules for the completion of work. The methodologies include the process of data collection, the method in which the data will be organized and analyzed. The methodology is based on the review, the methodologies are chosen appropriately. The data is collected with the help of the CSU library. The keywords that best defined the topic were chosen at the beginning of the work. The keywords such as blockchain,
healthcare monitoring, replication attack, security in wireless sensor networks, and many more that best suited the topic. The filters were restricted to the year 2020-2021 and the respected technology for selecting the 30 papers initially. Among the 30 Q1 selected papers, best 12 were selected for the review.

The research method used for the review is the secondary research method. The secondary research method collects the data from secondary sources such as research papers and journal articles related to the topic selected. The data is collected from secondary sources. The data is cited in the entire work along with the year of publishing. The research articles selected are published and provided a good source for the research work.

| TABLE I: COMPONENT TABLE |  |
|---------------------------|  |
| Factors | Attributes | Instances |
| Healthcare datasets | Decentralized dataset, Real-time dataset, Image processing dataset, medical dataset, organizational dataset, medical image dataset, e-healthcare dataset, central dataset, training dataset, private dataset, central repository dataset, arbitrary dataset, dynamic dataset, distribution model dataset, digital forensic dataset, heterogeneous dataset, botnet dataset, system log dataset, smartphone dataset, public utilities dataset, Haberman's survival dataset, human activity recognition dataset. |
| Data capturing devices | IoT devices, android devices, personal assisted device (PDA), wearable devices, blockchain-based IoT device, CT scan devices, MRI, radiology devices, X-rays, computerized tomography |
| Framework used | Deep learning-based framework, blockchain-based framework, truffle framework, medical service framework, disease classification framework, mobile edge computing framework, audit framework, network forensic framework, IoMT framework, healthcare data gateway framework, IoT framework, security framework, distribution system operator (DSO) framework, distributed computing framework, Health fog framework, privacy-preserving framework, GCN-MD framework, healthcare predictive modeling framework, data sharing framework, sulq framework, trust discovery framework. |
| Blockchain-based monitoring |  |
| Techniques | Deep learning techniques, data sharing techniques, data processing techniques, data enhancement techniques, data augmentation techniques, machine learning techniques, intelligent traceable techniques, blockchain techniques, cutting edge techniques, cryptographic techniques, data transmission techniques, active control techniques, IBS techniques, soft computing techniques, POS technique, privacy-preserving techniques, ELIB technique, clustering technique, consensus technique, partial private key (PPK) generation technique, public key generation technique, data quality evaluation technique, parallel computing technique |
| Algorithms | Bat algorithm, deep convolutional neural network algorithm, hospital registrations smart contract algorithm, uploading data using smart contract, training process of global model algorithm, intelligent optimization algorithm, swarm intelligence algorithm, multi-objective optimization algorithm, local search algorithm, batch algorithm, POX consensus mechanism algorithm, cryptographic algorithm, PBFT algorithm, POS algorithm, access rights and early warning threshold setting algorithm, Information upload algorithm, node consensus, forming blockchain algorithm, tampering with infectious disease information algorithm, tracing the infectious disease information of matching address algorithm, tracing the initial node from the finale node algorithm, hash function algorithm, machine learning algorithm, Euclidean distance algorithm, Jaccard distance algorithm, multilevel privacy guarantee algorithm, DBN algorithm, modified information dispersal algorithm (MIDA), traceability algorithm, asymmetric cryptographic algorithm, elliptic curve digital signature algorithm (ECDSA), NIST cryptographic algorithm, PoAh algorithm, Secure hash algorithm (SHA-256), signing algorithm, authsign algorithm, ReKeyGen algorithm, k-means algorithm, M-PPKS algorithm |
| Tools | New web tools, benchmark tool, memory utilization tool, simulation tool, network simulator 3, Cooj tool, remix tool, metamask tool, ganache tool, embark tool, populous tool, pyethereum tool, |
| Models | Deep learning model, global learning model, detection model, contour filter model, hybrid filtering model, CNN based model, AI-based deep neural network model, predictive model, detection model, resnet model, distribution model, network model, disease information tracing model, role-based access control (RBAC) model, factor model, MedRec model, data analysis model, smart grid healthcare system model, regression model, architectural model, random oracle model, MedHypChain model, security model, hyperledger fabric model, business model, machine-to-machine model, efficient lightweight |
Integrated blockchain (ELIB) model, cc model, trust model, GCN model, smart treatment model, threat model, graph model, MLP model, node detection model, big data model, graph neural network model, zero-knowledge proof (NIZK) model, k-means clustering analysis model

Healthcare system, interplanetary file system, remote patient monitoring system, cyber-physical system, community energy system, information and telecommunication system, big data sensing system, diverse health system, smart contract-based telesurgery system, deep learning system, ultrasound medical imaging system, electronic healthcare record system, botnet detection system, fast cp-abse system, traceability system, reliability system, disease direct reporting system, distributed systems, bookkeeping system, bitcoin direct currency system, blockchain system, operating system, hierarchical reporting system, smart grid healthcare systems, multiple diverse computing system, audit systems, eHealth system, forensics audit logging system, IoT system, industrial control system (ICS), surveillance system, fractional-order chaotic system, 3D jerk chaotic system

Deep neural network, blockchain decentralized network, recurrent convolutional neural network (RCNN), neural network, heterogeneous medical data network, RPN network, global network, P2P network, deep belief network, wireless sensor network, generative adversarial network (GAN), wireless multimedia sensor network, infrastructure storage network, wireless body area network, communication network, IoT network, blockchain network, IoT network, low power wireless personal area network (6LowPAN), graph neural network (GNN), healthcare network, large-scale distributed nodes network, anomalous network, transaction network, financial network, GuardHealth network

Malicious attack, blockchain-based security attack, 51% attack, single-point attack, database attack, data scavenging attack, untraceable attack, collusion attack, data masquerading attack, privileged insider attack, cyber-attack, chosen-message attack, forgery attack, middle attack, passive attack, DDoS attack, tampering attacks

Fault tolerance, mapping request, radial-gradient index, image data augmentation, data equalizer, hybrid filtering, smart contract addresses, byte, stochastic gradient descent (SGD), sampling layer, payoff, hop, computing power ratio, error cost function, loss value, access control mechanism, event rate, anonymity, power consumption, memory utilization, purity, NMI, trust value, recall, precision, throughput, frequency

Lesion detection, micro-calciﬁcation, blockchain-based cancer detection, deep learning detection, logistic regression-based detection, connection-based detection, behavioral malware detection, anomaly detection, malicious node detection, GCN based detection, edge detection

Event rate, density, analysis ratio, convolution layers, complex hash operations, hash values, hash functions, dimensional matrix (M), latency, loss-cl's and loss-box functions, accuracy, rotation-range, horizontal-Flip, shear-range, threshold value, PoX series consensus mechanism, estimator performance, synchronizing factor, anonymous distributed ledger, RAM, flash, clusters of instances, k-means methods, MedHypeChain performance, memory

### IV. CLASSIFICATION TABLE

The classification table explains the work of authors in a systematic and structured form to embed the understanding of the parameters that are used by the authors to define their work. The help was taken from the system component table. The attributes defined in the system component were taken as the base for explaining the work of different authors. The papers were deeply analysed and then the table was filled. The terms used by the authors to describe that attribute are mentioned in the system component that explains the effectiveness of the system components. The attributes such as healthcare dataset, data capturing devices, the framework used, techniques, algorithms, tools, and more are stated in the table, refer to table II for understanding.

### V. SYSTEM ARCHITECTURE

The evaluation table effectively helps in comparing the information based on the numerical values from the selected research articles. The numerical terms on the basis of the factors such as blockchain platform, throughput rate, latency, network, nodes, and more are stated in the table. The values that are filled in the table are searched in the articles and then stated in the table and some were derived based on the formulas stated in the research articles. The values are in the same measuring units for better comparison. The help is taken from the system components to select the basic factors for the table, refer to table III for the evaluation table. The comparison can be done as per the research articles.
| Authors | Healthcare datasets | Data capturing devices | Framework used | Techniques | Algorithms | Tools | Models | System | Networks | Attack Types | Data Type | Blockchain-based detection outcomes | Performance parameters |
|---------|---------------------|-----------------------|----------------|-----------|-----------|------|-------|--------|---------|-------------|----------|-----------------------------------|-----------------------|
| [28]    | Medical image dataset | CT scan devices | Deep learning-based framework | Deep learning techniques | Bat algorithm | New web tools | Deep learning model | Healthcare system | Decentralized network | Malicious attack | frequency | Lesion detection | Event rate |
| [75]    | N/A                 | IoT devices          | N/A            | N/A       |          |      |       |        |         |             |          | Fault tolerance | micro-calci| analysis ratio |
| [63]    | Knowledgeable dataset | wearable devices    | wearable devices | audit framework | intelligent traceable techniques | modified information dispersal algorithm (MIDA) | simulation tool | regression model | Security system | Infrastructure storage network | Scavenging attack | precision | logistic regression-based detection | hash functions |
| [48]    | botnet dataset      | wearable devices     | audit framework | knowledgeable | machine learning techniques | machine learning algorithm | data analysis tool | audit systems | Deep belief network | Data loss throughput |       | deep learning detection | hash values |
| [27]    | N/A                 | personal assisted device (PDA) | personal assisted device | indexing algorithm | Embark tool | random oracle model | Data sharing system | Wireless body are network | Security attack | recall | deep learning detection | latency |
| [31]    | organizational dataset | blockchain-based IoT device | blockchain-based IoT framework | cryptographic techniques | ARM Cortex M4 processor | Business model | IoT system | IoT network | Cyber attack | trust value | connection-based detection | accuracy |
| [35]    | Real-time dataset   | radiology devices    | security framework | active control techniques | Probabilistic algorithm | random oracle model | Chaotic system | Wireless body are network | Chosen-message attack | byte | malicious node detection | estimator performance |
| [39]    | central dataset     | wearable devices     | distribution system operator (DSO) framework | POS technique | Consensus algorithm | Electronic medical recording tool | Authentication system | Overlay network | Man-in-middle attack | computing power ratio | behavioural malware detection | anonymous distributed ledger |
| [55]    | Medical dataset     | X-ray                | distributed computing framework | clustering technique | Regression tree algorithm | IoT based tools | Diverse recognition system | Neuro-fuzzy network | N/A | Precision | edge detection | F1-measure |
| [71]    | Data transaction dataset | wearable devices    | blockchain framework | Evaluation technique | logistic regression model | N/A | MLP model | Blockchain system | Graph neural network (GN) | Active attack | frequency | anomaly detection | clusters of instances |
| [70]    | training dataset    | android devices      | blockchain framework | POS algorithm | trust model | Medical system | P2P network | Countering tampering attack | smart contract addresses | deep learning detection | hash functions |
| [17]    | Smartphone dataset  | Sensor device        | IoT framework | parallel computing technique | k-means algorithm | N/A | k-means clustering analysis model | Healthcare system | Wireless sensor network | Resist collusion attack | N/A | anomaly detection | Recall |
VI. SYSTEM ARCHITECTURE

![System Architecture Diagram]

Fig. 1. Overview of System Architecture. Source: Deng (2020).
VII. RESULTS

The review of Blockchain-based intelligent monitoring system for detection of replication attack in the wireless healthcare network. The results from the work are as follows:

The advancement of the internet of things has revolutionized the way healthcare works these days. Reference [48] explained that wireless healthcare networks have provided a platform to connect different sensor nodes to the healthcare monitoring system for efficiently monitoring the patient’s data. Blockchain has bought various advancements, applicability, and authorization in the field of technology. Blockchain has various benefits one of which is providing security to the system and data. Reference [35] explains that blockchain technology has made it easier and reliable for healthcare systems especially monitoring systems in providing security to the healthcare system.

The system component table that was proposed in the research work is based on the overall understanding of the articles that were initially selected for the review. The system component explains the insights and understanding about the process steps that are input-process-output-evaluation. Based on these process steps the factors-attributes, and the instances are defined in the system component table. The system component table can be verified with the help of the percentage graph and theoretical description of the term frequency used in the work. The verification of the system component with the help of system verification, explains the terms that are used in the work with the help of the percentage of the terms used. The general understanding behind this is to state the usefulness of the system component and verify whether it is useful or not. The terms selected are from the instances and attributes of the system component table. It states the completeness of the work, as how many authors have used the term. The more the percent the more effective is the system component table. This process cannot be achieved using any software or any specific tool as this is completely based on context-dependency, this masked it difficult to automate the process, refer to Fig. 1. For example, the term data is used by 80% of authors to state the input in the system and 75% of authors stated the term healthcare dataset.

| TABLE IV: TERM FREQUENCY |
|--------------------------|
| Term     | Frequency | Term      | Frequency |
| Dataset   | 70         | Framework | 100        |
| Technique | 100        | Algorithm | 310        |
| Models    | 322        | Systems   | 566        |
| Network   | 478        | Attack    | 125        |
| Detection | 129        | Security  | 436        |
| Blockchain| 931        | Healthcare| 577        |

The completeness and usefulness of the system component can be verified with the help of the term frequency table. This depicts the theoretical analysis of the system component table, refer to Table IV. The most frequently used terms are selected from the system component. The terms are thoroughly checked in the selected 12 articles for the analysis of the terms selected. The frequency of the terms is stated in the table. The higher the frequency the more effective the system component table. The frequency here refers to the appearance of the term in the paper.

VIII. DISCUSSION

The work explains the review of blockchain-based intelligent monitoring systems for the detection of replication attacks in wireless healthcare networks. Based on the work of the authors that were initially selected, the system component table and system classification table are prepared that define the factors, attributes, and instances of the work of different authors. The component table explains the important factors related to the topic. The factors were selected such that they explain the input-processing-evaluation-output of the work.

A. Healthcare Data

The factors such as healthcare data that is a factor that states the datasets used in the work, the second attribute is data capturing devices that explain the devices that are used in healthcare monitoring that is a source of input in the system, the framework used in other attributes that define the input step.

B. Blockchain-based Monitoring

Blockchain-based monitoring is the factor that states the processing step of the system. The attributes such as techniques, algorithms, tools, models, systems, and network attributes. These attributes are used for the processing of the work. The instances define the different approaches by the authors.

C. Attack Detection

The next factor is attack detection that explains the evaluation step that is the attributes of this factor explain the different approaches used for the evaluation such as the attributes are attack types, data type, and blockchain-based detection outcomes.

D. Evaluation

The last step is the evaluation that states the outcomes of the work, the attribute in the evaluation is performance parameters that explain the outcomes of each of the works of authors after the completion of the process.

System classification tables explain each of the instances that are defined in the component table corresponding to the

Fig. 2. Percentage of component.
authors. The classification table explains the components stated in the component tables as per the literacy work of the authors. The information provided in the component table helps in understanding the different attributes that are used in the work. The component table provides an overview of the different techniques, algorithms, frameworks, tools, and other parameters and components that are used for the detection of replication-based attacks in the healthcare system. The blockchain techniques and algorithms along with other parameters can be viewed in one place. The work of the authors can be analyzed with the help of the classification table.

IX. CONCLUSION

Wireless sensor networks have gained a lot of attention from various sectors for implementing the technology for the betterment of the sector. One such sector is the healthcare sector. The implementations of wireless sensor networks have eased down the monitoring of healthcare systems. The open nature of wireless channels makes the system vulnerable to threats. These threats pose security issues related to the privacy and confidentiality of the data. Replication attacks make replicas of the node, infuse them with the malicious data and deploy them in the network in place of the original node. Replication attacks go undetected because of their properties. This issue is solved using blockchain-based monitoring systems. The aim of the work was to review the Blockchain-based intelligent monitoring system for the detection of replication attacks in the wireless healthcare network. Blockchain technology brings various advantages to the data and system. Blockchain provides security to the data and eliminates such risks and threats. The proposed system component is verified graphically and theoretically. Through the above-held review, it can be concluded that a blockchain-based intelligent monitoring system can be used for the detection of replication attacks in wireless healthcare networks as it provides security to the data and the system. The technology in the future can be used in other domains as well for security and privacy challenges.

APPENDIX

| Abbreviations | Description |
|---------------|-------------|
| IoT           | Internet of things |
| M-PPKS        | Mutual privacy-preserving k-means strategy |
| ELIB          | Efficient Lightweight Integrated |
| WSN           | Blockchain |
| DDoS          | Distributed Denial-of-Service |
| ECG           | Electrocardiogram |

REFERENCES

[1] Abuekhalil, U. Baroudi, M. Raad, and T. Sheltami, “Internet of things for healthcare monitoring applications based on RFID clustering scheme,” Wireless Networks, vol. 27, no. 1, pp. 747–763, Nov. 2020, doi: 10.1007/s11276-020-02482-1.

[2] Y. Al-Handarsh et al., “A Survey of Tactile-Sensing Systems and Their Applications in Biomedical Engineering,” Advances in Materials Science Engineering, pp. 1–18, Jan. 2020, doi: 10.1155/2020/4047937.

[3] M. M. Alhejazi and R. M. A. Mohammad, “Enhancing the blockchain voting process in IoT using a novel blockchain Weighted Majority Consensus Algorithm (WMCA),” Information Security Journal: A Global Perspective, pp. 1–19, Jan. 2021, doi: 10.1080/19393555.2020.1869356.

[4] Barredo Arrieta et al., “Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI,” Information Fusion, vol. 58, pp. 82–115, Jun. 2020, doi: 10.1016/j.inffus.2019.12.012.

[5] S. Balasubramanian, V. Shukla, J. S. Sethi, N. Islam, and R. Saloum, “A readiness assessment framework for Blockchain adoption: A healthcare case study,” Technological Forecasting and Social Change, vol. 165, p. 120536, Apr. 2021, doi: 10.1016/j.techfore.2020.120536.

[6] E. Bandara, D. Tosh, P. Foytik, S. Shetty, N. Ranasinghe, and K. De Zeya, “Tikiri—Towards a lightweight blockchain for IoT,” Future Generation Computer Systems, vol. 119, pp. 154–165, Jun. 2021, doi: 10.1016/j.future.2021.02.006.

[7] U. A. Bhatti et al., “Predictive Data Modeling Using sp-kNN for Risk Factor Evaluation in Urban Demographic Healthcare Data,” Journal of Medical Imaging and Health Informatics, vol. 11, no. 1, pp. 7–14, Jan. 2021, doi: 10.1166/jmihi.2021.3313.

[8] M. Bhowmik, S. Chakraborty, S. Tripathi, S. Tyagi, and N. Kumar, “Blockchain and quantum blind signature-based hybrid scheme for healthcare 5.0 applications,” Journal of Information Security and Applications, vol. 56, p. 102673, Feb. 2021, doi: 10.1016/j.jisa.2020.102673.

[9] M. Chen et al., “Blockchain-Enabled healthcare system for detection of diabetes,” Journal of Information Security and Applications, vol. 58, p. 102771, May 2021, doi: 10.1016/j.jisa.2021.102771.

[10] M. Ciampi, A. Esposito, F. Marangio, M. Sicuranza, and G. Schmid, “Modernizing Healthcare by Using Blockchain,” Studies in Big Data, pp. 29–67, Dec. 2020, doi: 10.1007/978-981-15-9547-9_2.

[11] J. Deng, J. Cai, M. U. Aftab, M. S. Khokhar, and R. Kumar, “Visual Features with Spatio-Temporal-Based Fusion Model for Cross-Dataset Vehicle Re-Identification,” Electronics, vol. 9, no. 7, p. 1083, Jul. 2020, doi: 10.3390/electronics9071083.

[12] S. Deokar, M. Mangla, and R. Akhare, “A Secure Fog Computing Architecture for Continuous Health Monitoring,” Fog Computing for Healthcare 4.0 Environments, pp. 269–290, Aug. 2020, doi: 10.1007/978-3-030-46197-3_11.

[13] R. K. Dwivedi, R. Kumar, and R. Buyya, “Gaussian Distribution-Based Machine Learning Scheme for Anomaly Detection in Healthcare Sensor Cloud,” International Journal of Cloud Applications and Computing, vol. 11, no. 1, pp. 52–72, Jan. 2021, doi: 10.4018/jicac.2021011013.

[14] H. B. Elhadi, F. Sallali, A. Henaïne, L. Chaari, K. Shuaib, and M. Al Thawadi, “Do-Care: A dynamic ontology reasoning based healthcare monitoring system,” Future Generation Computer Systems, vol. 118, pp. 417–431, May 2021, doi: 10.1016/j.future.2021.01.001.

[15] L. Erhan et al., “Smart anomaly detection in sensor systems: A multi-perspective review,” Information Fusion, vol. 67, pp. 64–79, Mar. 2021, doi: 10.1016/j.inffus.2020.10.001.

[16] L. Fang, Y. Li, Z. Liu, C. Yin, M. Li, and Z. J. Cao, “A Practical Model Based on Anomaly Detection for Protecting Medical IoT Control Services Against External Attacks,” IEEE Transactions on Industrial Informatics, vol. 17, no. 6, pp. 4260–4269, Jun. 2021, doi: 10.1109/TII.2020.3011444.

[17] X. Guo, H. Lin, Y. Wu, and M. Peng, “A new data clustering strategy for enhancing mutual privacy in healthcare IoT systems,” Future Generation Computer Systems, vol. 113, pp. 407–417, Dec. 2020, doi: 10.1016/j.future.2020.07.023.

[18] M. Gupta, R. Jain, M. Kumari, and G. Narula, “Securing Healthcare Data by Using Blockchain,” Studies in Big Data, pp. 93–114, Dec. 2020, doi: 10.1007/978-981-15-9547-9_4.

[19] M. Ul Hassan, M. H. Rehmani, and J. Chen, “Differential privacy in blockchain technology: A futuristic approach,” Journal of Parallel and Distributed Computing, vol. 145, pp. 50–74, Nov. 2020, doi: 10.1016/j.jpdc.2020.06.003.

[20] Hasselgren, K. Kralevska, D. Gligoroski, S. A. Pedersen, and A. Faxvaag, “Blockchain in healthcare and health sciences—A scoping review,” International Journal of Medical Informatics, vol. 134, Feb. 2020, doi: 10.1016/j.ijmedinf.2019.104040.

[21] H. Huang, P. Zhu, F. Xiao, X. Sun, and Q. Huang, “A blockchain-based scheme for privacy-preserving and secure sharing of medical data,”
[60] Surantha, T. F. Lesmana, and S. M. Isa, “Sleep stage classification using extreme learning machine and particle swarm optimization for healthcare big data,” Journal of Big Data, vol. 8, no. 1, pp. 1–17, Jan. 2021, doi: 10.1186/s40537-020-00406-6.

[61] Tandon, A. Dhir, N. Islam, and M. Mäntymäki, “Blockchain in healthcare: A systematic literature review, synthesizing framework and future research agenda,” Computers in Industry, vol. 122, pp. 1–22, Nov. 2020, doi: 10.1016/j.compind.2020.103290.

[62] M. Tanniru, J. Niu, C. Feng, C. G. Duque, C. Lu, and H. Krishnan, “Incentives to Engage Blockchain and Ecosystem Actors,” Building Decentralized Trust, pp. 35–61, 2021, doi: 10.1007/978-3-030-54414-0_3.

[63] Tolba and Z. Al-Makahdmeh, “Predictive data analysis approach for securing medical data in smart grid healthcare systems,” Future Generation Computer Systems, vol. 117, pp. 87–96, Apr. 2021, doi: 10.1016/j.future.2020.11.008.

[64] S. Tuli, N. Basumatary, and R. Buyya, “EdgeLens: Deep Learning based Object Detection in Integrated IoT, Fog and Cloud Computing Environments,” 2019 4th International Conference on Information Systems and Computer Networks (ISCON), pp. 496–502, Nov. 2019, doi: 10.1109/isccon47742.2019.9036216.

[65] S. Tuli et al., “HealthFog: An ensemble deep learning based Smart Healthcare System for Automatic Diagnosis of Heart Diseases in integrated IoT and fog computing environments,” Future Generation Computer Systems, vol. 104, pp. 187–200, Mar. 2020, doi: 10.1016/j.future.2019.10.043.

[66] S. Tuli, R. Mahmud, S. Tuli, and R. Buyya, “FogBus: A Blockchain-based Lightweight Framework for Edge and Fog Computing,” Journal of Systems and Software, vol. 154, pp. 22–36, Aug. 2019, doi: 10.1016/j.jss.2019.04.050.

[67] M. Uddin, “Blockchain Medledger: Hyperledger fabric enabled drug traceability system for counterfeit drugs in pharmaceutical industry,” International Journal of Pharmaceutics, vol. 597, Mar. 2021, doi: 10.1016/j.ijpharm.2021.120235.

[68] M. Vahdati, K. Gholizadeh HamlAbadi, and A. M. Saghiri, “IoT-Based Healthcare Monitoring Using Blockchain,” Studies in Big Data, pp. 141–170, Dec. 2020, doi: 10.1007/978-981-15-9547-9_6.

[69] M. Vahdati, K. Gholizadeh HamlAbadi, and A. M. Saghiri, “IoT-Based Healthcare Monitoring Using Blockchain,” Studies in Big Data, pp. 141–170, Dec. 2020, doi: 10.1007/978-981-15-9547-9_6.

[70] Z. Wang, N. Luo, and P. Zhou, “GuardHealth: Blockchain empowered secure data management and Graph Convolutional Network enabled anomaly detection in smart healthcare,” Journal of Parallel and Distributed Computing, vol. 142, pp. 1–12, Aug. 2020, doi: 10.1016/j.jpdc.2020.03.004.

[71] Z. Wu et al., “MD-NDNet: a multi-dimensional convolutional neural network for false-positive reduction in pulmonary nodule detection,” Physics in Medicine & Biology, vol. 65, no. 23, Dec. 2020, doi: 10.1088/1361-6560/aba87c.

[72] Yaqoob, K. Salah, R. Jayaraman, and Y. Al-Hammadi, “Blockchain for healthcare data management: opportunities, challenges, and future recommendations,” Neural Computing and Applications, pp. 1–16, Jan. 2021, doi: 10.1007/s00521-020-05519-w.

[73] Zhu, J. Hu, Y. Zhang, and X. Li, “Enhancing Traceability of Infectious Diseases: A Blockchain-Based Approach,” Information Processing & Management, vol. 58, no. 4, pp. 1–20, Jul. 2021, doi: 10.1016/j.ipm.2021.102570.