A Secure and Transparent Communication Mechanism based on Blockchain and Fuzzy Evaluation Matrix in Metaverse Industry 4.0

Chaker Abdelaziz Kerrache[a,*], Geetanjali Rathee[b], Mohamed Lahby[c], Anna Maria Vegni[d], Muhammad Bilal[e], Mohamed Amine Ferrag[f]

[a] Laboratoire d'Informatique et de Mathématiques, Université de Laghouat, 03000 Laghouat, Algeria.
[b] Department of Computer Science and Engineering, Netaji Subhas University of Technology, Dwarka Sector-3, New Delhi-110078, India.
[c] Hassan 2 University, ENS Casablanca, Morocco.
[d] Department of Engineering, Roma Tre University, Italy.
[e] Department of Computer and Electronics Systems Engineering, Lancaster University, Lancaster, UK.
[f] Technology Innovation Institute, 9639 Masdar City, Abu Dhabi, United Arab Emirates.
[*] Corresponding author: Chaker Abdelaziz Kerrache (ch.kerrache@lagh-univ.dz)

ARTICLE HISTORY
Compiled May 18, 2024

ABSTRACT

Recently, Metaverse is gaining prominence within the field of radiology due to its potential to revolutionize image visualization. Radiologists can harness its capabilities to access dynamic, highly detailed results, thereby enhancing diagnostic precision. Digital twins, at the core of the Metaverse, are digital replicas of real-world objects and entities. They serve as the foundational building blocks, enabling the creation of virtual counterparts for everything within the Metaverse. To ensure the reliability of these digital twins, blockchain technology offers a multi-dimensional data storage solution, reinforcing data integrity and trustworthiness. It is used to ensure a transparent and 3D visualization of each communication and interaction for further looking up any criticality if present in the network. With the rapid increase in value and volume of data, the evolution of metaverse faces number of privacy and security concern. Further, the metaverse in Industry 4.0 is trending topic that further needs to focus on their security challenges at its initial stage. Fortunately, blockchain is considered as one of the significant solutions.

KEYWORDS
Metaverse; Security; Industry 4.0; Metaverse Applications; Secure Industry 4.0; Blockchain, Fuzzy evaluation matrix, Trust Mean Aggregation Method

1. Introduction

Metaverse is considered as the future of Internet where an immersive and universal virtual world, facilitated by the Augmented Reality (AR) and Virtual Reality (VR), coexist (Wohlgenannt et al., 2020). The metaverse is termed as a virtual environment where physical world overlaps with the virtual surroundings where people converse through digital avatars.

The rapid progress in automation and digitalization have led to a significant growth in various applications by creating new channels for rendering the efficient

and effective communications. The metaverse influences multiple technologies in several applications such as Healthcare sectors, smart cities, Industry 4.0, intelligent transportation system to provide new directions for exploring high-data rate services and communications. Recent applications involve new mechanisms for promoting and ensuring an effective communication without human intervention.

Industry 4.0 (Ghobakhloo, 2020) is considered as one the significant determinant of metaverse for ensuring physical, general, mental and social well-being of the entire population in the world. The major objective of Industry 4.0 is to channelize the efforts towards a number of activities that restore, promote, improve and maintain the communication services. It also contributes massively towards significant development in country industrialization and economy.

The metaverse may also helps the manufacturers to look into any defect or repair of a machine instead of manually looking and putting your life into danger. The use of digital twins in the metaverse will keep the manufacturers well engaged and informed before any mishap wherein manufacturers, stakeholders and vendors are integrated to develop a digital simulation of the industry (Guo et al., 2021; Prinsloo et al., 2019). Digital twins are defined as the building blocks of the metaverse by creating digital replica of every single object in the metaverse (Clim, 2019).

1.1. Need of Security in Metaverse

Though the combination of various characteristics provides a new level of communication and mapping among the real and digital world, it also makes the present privacy and security issues in more critical ways (Mystakidis, 2022; Y. Wang et al., 2022). Security issues include hacking personal and sensitive information leakage through Brain Computer Interface (BCI), where intruders may hack the real world by connecting it through the metaverse. In addition, the main characteristics of the metaverse not only provide a fantastic or novel digital world but also make it suffer from several security and privacy concerns, such as broken authentication, eavesdropping, personal information leakage, data injection, unauthorized access and so on. Metaverse is in its early stage and needs to focus on several security concerns (Anthes et al., 2016; Kniaziev, 2017). Therefore, it is needed for engineers, entrepreneurs, and researchers to understand and discuss the impact of upcoming resolutions. Though various researchers/scientists have proposed several security methods and trusted schemes, they all focus on reliability, optimization, and network performance enhancement metrics such as throughput, delay, information loss, etc. Implementing security methods while sharing, decision-making, and ensuring accuracy and transparency in the system is still in its early stages.

The concept of blockchain in the metaverse is fundamental as the centralized data storage and its analysis mechanisms may cause several privacy, security, and data transparency issues in the network (Yaga et al., 2019). The blockchain in the metaverse makes a decentralized digital source and lets people access or share any information without the involvement of any centralized authority. The decision-making and high-quality authenticity will be much easier using blockchain (X. Li et al., 2020).

Figure 1 depicts the overview of blockchain-assisted industry 4.0 (L. Li et al., 2018) in the metaverse, which ensures a secure and efficient communication process. The depicted Figure 1 illustrates Industry 4.0 application in metaverse where the communication process. At the same time, manufacturing, shipping, supply chain, recording, and analysis of information can be easily traced and maintained through blockchain by further storing it on online servers. In addition, the complete blockchain-assisted system can be merged with the metaverse in order to provide efficient communication with reduced costs and efforts.

1.2. Motivation

By introducing virtual technologies in a real-world environment, the metaverse goal is to provide excellent user interaction and experience for people or business organizations in a virtual world by interconnecting the physical world virtually. In addition, the metaverse can gather personal and sensitive information such as data recordings, generations, analysis, raw material data, data storage, etc. The information from such recordings is unsafe in the virtual world as several persons interact

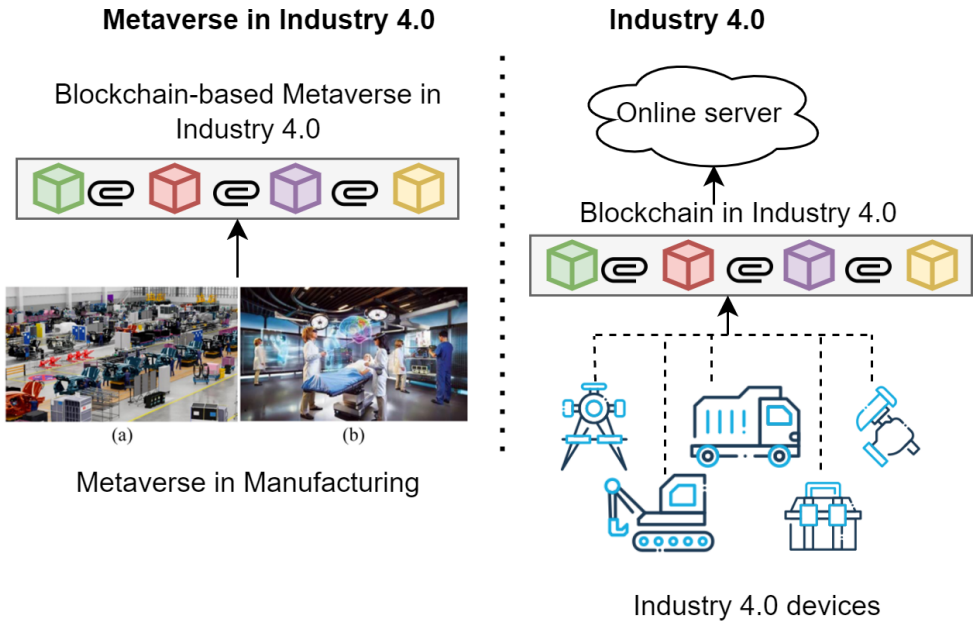

Figure 1. Schematic of Metaverse in Industry 4.0.

and communicate, thus causing increasing interference. The number of intruders may imitate the users for stealing the personal information of individuals or even compromise the IoT devices in the network. Further, by considering the case of Industry 4.0, where the electronic generation of information having personal and sensitive information related to raw materials, shipping orders, manufacturing, and securing such information from external attackers or breaches at distinct levels is considered as one of the challenging tasks.

1.3. Our Contributions

This manuscript aims to propose a transparent and secure communication process in Industry 4.0 through blockchain and fuzzy evaluation matrix (FEM) based on the trust mean aggregate method, and we discuss its various potential applications.

In this paper, Kang et al. have considered the contract theory (Kang, Xiong, Niyato, Xie, et al., 2019; Kang, Xiong, Niyato, Ye, et al., 2019) an accurate and efficient security mechanism used for predicting vehicular transmission situations. We have used this approach to predict an accurate decision-making task, analyze records generated by the real-world environment, and map it with the virtual world. The proposed mechanism is validated against security concerns such as broken authentication, eavesdropping, personal information leakage, data injection, and unauthorized access.

Below, we briefly explain the contributions of our study in two points:

A Fuzzy Evaluation Matrix based on the Trust Mean Aggregation Scheme mechanism is used to predict the FEM accuracy of devices in the network. In addition, FEM is used for predicting accurate decision-making and analysis of records generated by the system;
The blockchain technology is integrated with FEM to maintain transparency among devices in the network.
By combining the devices' fuzzy trust value and blockchain mechanism, the proposed mechanism is validated against a traditional approach when considering various security metrics, including broken authentication, eavesdropping, personal information leakage, data injection, and unauthorized access.

The overall structure of the paper is discussed as follows. Section 2 deliberates the literature survey of various approaches proposed for ensuring a secure and effi-

cient communication mechanism in metaverse systems. The proposed mechanism is discussed in Section 3 with the proper pseudocode and the system model. The performance analysis for validating the proposed framework is discussed in Section 4. Finally, conclusions are drawn at the end of the paper.

2. Related Work

To provide excellent user interaction and gain experience in integrating the virtual world with the real-world environment, it is necessary to establish an efficient, secure, and transparent communication system. This section illustrates various security schemes and methods proposed by researchers and scientists for providing a secure metaverse system using cryptography-based schemes. Chen et al. (Chen et al., 2022) have presented several security concerns for developing technologies related to the metaverse. They have discussed security-related issues in various metaverse applications and suggested some solutions. The authors have also raised several open challenges in the potential metaverse, surveying in-depth issues on security and privacy risks and providing insightful directions for further research.

Huang *et al.* (Huang et al., 2023) have discussed the characteristics of the metaverse by categorizing them into various sectors. The authors have discussed current progress along with some privacy and issues concerns in the metaverse. They have addressed potential issues raised after combining these characteristics and introduced some concerns related to humanity and society in metaverse applications. Chengoden *et al.* (Chengoden et al., 2023) have provided a comprehensive survey on healthcare issues in the metaverse. They have emphasized various security issues, the state of the art, related projects, enabling technologies, and potential applications. The authors have discussed metaverse adoption issues, plausible solutions, and future research directions. Fu *et al.* (Fu et al., 2022) have discussed the development characteristics, trends, and frameworks of the metaverse. Additionally, they have illustrated existing work on the metaverse using blockchain by examining challenges and applications. Furthermore, they have summarized metaverse applications by emphasizing various developments in metaverse security fields. Moreover, they have discussed challenges, open issues, and future directions. Huamanchahua *et al.* (Huamanchahua et al., 2022) have reviewed immersive technology in the field of Industry 4.0. They discussed implementation aspects and investigations on various platforms, devices, and software to compact the S3 models. Nguyen *et al.* (Nguyen et al., 2022) have proposed a Meta-chain blockchain-based architecture for addressing security concerns in metaverse applications. The proposed framework efficiently manages and automates interactions with providers and metaverse users. Additionally, the authors have used a novel sharing mechanism to improve blockchain scalability.

Lippet *et al.* (Lippert et al., 2021) have presented metaverse design by adopting a global approach to communication. They have proposed an AI-driven model by deploying model-based systems in the future. The authors have further offered various open research questions that academia must address to further improve communications in the future metaverse. Kim *et al.* (Kim & Oh, 2022) have investigated the challenges and opportunities of the metaverse in mobility and automotive fields. They have explored the metaverse structure, concept, and technical requirements of networking and wireless communication systems. The authors have also illustrated and proposed various ideas for industries by analyzing their challenges and opportunities. Bansal *et al.* (Bansal et al., 2022) presented the first comprehensive survey examining metaverse developments in healthcare applications. They have covered various domains to profoundly understand the concept. The authors have developed a self-sustained, persistent, and future-proof solution for the medical healthcare system, highlighting various challenges in embracing the metaverse in the healthcare sector. Zonaphan *et al.* (Zonaphan et al., 2022) have illustrated a systematic review for discovering learning in the metaverse. The authors have concluded the effective learning tools of the metaverse by defining their advantages. They have discussed various limitations in tools that support the metaverse and have maximized the full advantage by handling multiple limitations of the learning platform. Dutkiewicz and Nguyen have developed an effective and efficient framework based on a semi-Markov model and decision process on intelligent systems. The authors have proposed an intelligent algorithm for maximizing resource utilization and enhancing the quality of service for end-users. Table 1 summarizes the main security solutions for metaverse

applications.

Table 1. Recent work on Security in Metaverse Application

Authors	Technique	Definition	Limitation
Chen et al. (Chen et al., 2022)	Development of technologies related to metaverse	Various applications of metaverse with the scope of some solutions.	Delay in real time analysis
Huang et al. (Huang et al., 2023)	Characteristics of metaverse	current progress along with some privacy and issues concerns	Online overhead
Chengoden et al. (Chen et al., 2022)	Comprehensive survey on healthcare issues	Emphasized on various security issues, state of art, related projects	Calculation delay
Lippet et al. (Lippert et al., 2021)	design of metaverse	proposed a AI-driven model by deploying the model-based systems	Communication latency
Kim et al. (Kim & Oh, 2022)	investigated the challenges and opportunities of metaverse	Explored the metaverse structure, concept and technical requirements	Higher trust issues
Zohaphan et al. (Zonaphan et al., 2022)	Illustrated a systematic review for discovering the learning	Concluded the effective learning tools of metaverse	Computational latency

Overall, despite researchers projecting various mechanisms and schemes, most of them focused solely on computational and storage overhead issues. Furthermore, very few have focused on providing a secure communication mechanism. This paper presents a secure and trusted communication system while reducing computational and storage overhead in the environment. Additionally, although numerous ML-based cryptographic mechanisms are already proposed by several scientists, existing mechanisms lack accuracy, storage overhead, and key management (Lakhan, Mohammed, Abdulkareem, et al., 2024; Lakhan, Mohammed, Zebari, et al., 2024; Mohammed et al., 2024). The proposed mechanism integrates the Fuzzy Evaluation Matrix with a trust-based scheme to analyze the internal working of communicating devices accurately with less delay and storage overhead. Furthermore, a blockchain mechanism is used to ensure real-time security in processing and information processing.

3. Proposed Approach

The system model of the proposed framework is presented in Figure 2, having several devices for performing various tasks such as manufacturing, shipping chain, recording, analysis, and supply chain. The proposed framework uses blockchain and fuzzy evaluation matrix (FEM) to ensure a secure communication framework with transparency, high reliability, and prediction. The fuzzy evaluation matrix can effectively recognize malicious IoV devices' involvement by analyzing the network's transmitting information. The trust value computation analyzes the generated/collected reports from each IoV device and records the accuracy and reliability of the transmitting information. Here, the FEM mechanism is used to examine the reports in

the network. In addition, the blockchain maintains surveillance on the devices by ensuring a transparent communication framework. The detailed explanation of FEM and blockchain in Industry 4.0 is texted below.

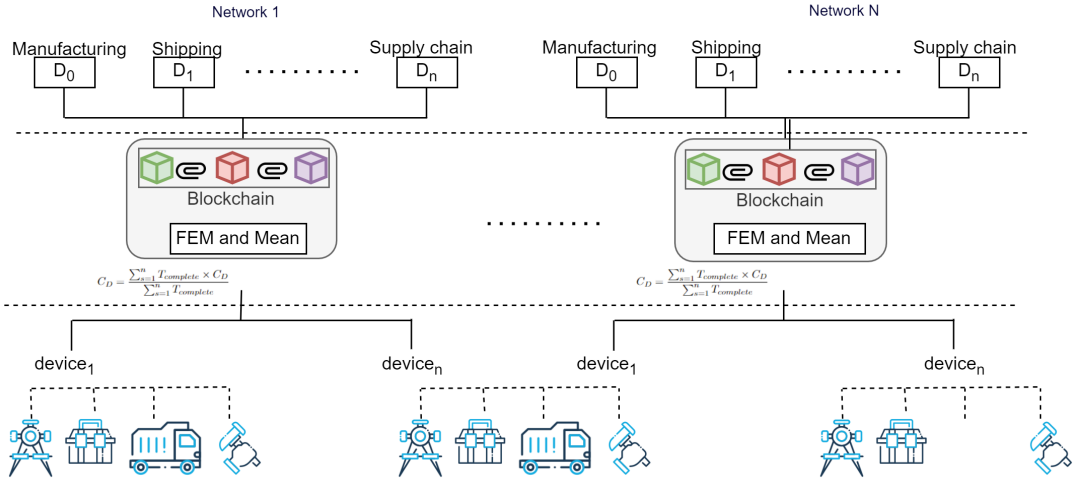

Figure 2. Proposed Security Framework.

3.1. Fuzzy Evaluation Matrix based on Mean Aggregation Scheme

Numerous cryptographic schemes have been proposed by various researchers and scientists; however, these schemes increased storage overhead, key management overhead, or computational complexities while ensuring security in the network. Trust-based mechanisms such as subjective logic, direct indirect method, recommendation system, fuzzy evaluation matrix (FEM) can be easily replaced by cryptographic schemes to avoid the above said limitations. The proposed framework uses a trusted scheme such as FEM that provides accurate decision-making in real-time. The FEM matrix is accurate compared to other trusted schemes as device trust is not only computed by a single device but is dependent on, analyzed, and evaluated based on their neighbors' trust evidence by checking their past history progress.

To validate whether the devices are analyzing, gathering, and recording the information properly, the accuracy, decision-making, and precision of the data are analyzed using FEM. The trust of the computed device not only depends on the evidence but also affects or influences the neighboring devices to rely on the computed trust, which further affects the authorization accuracy. The evidence of trust set as $Trust_E$ can be defined as:

$$Trust_E = e_1; e_2; :::e_x \tag{1}$$

Where $e_1; e_2; :::e_x$ are the trust evidences from various devices. In addition, the trust degree $Trust_{degree}$ of each evaluated level set is illustrated as follows:

$$Trust_{degree} = d_1; d_2:::d_y \tag{2}$$

Where $d_1; d_2:::d_y$ is the degree of trust from various devices.

The fuzzy evaluation matrix is identified after selecting the Trust evidence (TE) and Trust degree (TD) as $FEM = (\ _{ij})_{xy}$, which is defined as the membership degree of TE_i to TD_j. Now, after selecting the trust degrees and trust levels of each communicating device in the network, the weights are assigned to each device for identifying the entropy or communicating behavior of n^{th} evidence as follows:

$$TE_n = \frac{1}{ln_y} \sum_{j=1}^{X} {}_{ij} ln(\ {}_{ij}) \tag{3}$$

$${}_{ij} ln(\ {}_{ij}) = 0;\ \ {}_{ij} = 0 \tag{4}$$

The weight values are further derived from TE as:

$$W_n = \frac{1 \quad \sum_{i=1}^{x} TE_n}{n \quad TE_n} \tag{5}$$

Where W_n is within [0 1] and $TE_n = 1$ (J. Wang et al., 2017). To correct the weight vectors for further improving the accuracy, the weight vector (WV) is defined as:

$$WV_x = w1; w2; ::::w_x \tag{6}$$

Where $w1; w2; ::::w_x$ are the weights of the different devices.

Now, the computation of trust based upon evidence-set values is defined as the quantization level. Trust degree of each evaluated level set as $Trust_{degree}$ corresponding to quantization value set QL is illustrated as:

$$QL = q1; q2; :::q_x \tag{7}$$

Where $q1; q2; :::q_x$ represent the quantization value of the different devices.

Now, based upon evidence level and trust degree factors (J. Wang et al., 2017), the present device trust value can be computed as:

$$T_{PR} = \frac{\sum_{p=1}^{q} QL_n \quad EV_n}{\sum_{p=1}^{q} EV_n} \tag{8}$$

The evaluation vector $EV_n = ev_1; ev_2; :::ev_m$ is derived from the compound operation concerning weight vector WV and matrix M. The average trust value of each device based upon its history is defined as:

$$T_{previous} = \frac{1}{z} \sum_{f=1}^{X} TPR_f \ \ (f) \tag{9}$$

Where f belongs to $[1; z]$, where (f) is an attenuation function to reduce the impact of earlier records of trust history while computing the trust value. The complete trust value after checking their evidence and previous records is defined as:

$$T_{complete} = \ T_{PR} + \ T_{previous} \tag{10}$$

Where $+ = 1$ depends on specific conditions. Now, as each device D has n different sources of information for suggesting the trust value of an unknown quantity K. The device D should aggregate the obtained values from multiple sources. Now, if each source s reports value C_s as a convinced value for K and D trusts each s with complete trust value $T_{complete}$, then the aggregation result C_D, i.e., the value that D believes for K is defined as:

$$C_D = \frac{\sum_{s=1}^{n} T_{complete} \quad C_D}{\sum_{s=1}^{n} T_{complete}} \tag{11}$$

3.2. Blockchain Incorporation

The proposed framework integrates a private blockchain mechanism as a backend by keeping the information private and sensitive to compete with rival industries. A private blockchain is one where storing, accessing, and modifying any single piece of information is attained at various levels without sharing among each other without the permission of an administrator. Here, a separate blockchain is maintained for multiple processes, such as storing records, manufacturing products, and delivering items. All blockchain networks are monitored and maintained by the administrator. Furthermore, the blockchain is integrated with the proposed framework by relying on Java where blockchain creation, insertion, and validation are implemented easily. The blockchain contains the creation module responsible for creating each block using its previous and current hashes. Additionally, for information insertion, devices can add several records in the network. Here, we have inserted raw material to analyze its efficiency.

Furthermore, newly added blocks are maintained through miners for proper verification and validation. If miners successfully verify the block, then the block is considered ideal or altered. Initially, a block of 4 ledgers is implemented using a hyper ledger where each block contains the product record with their respective hashes. The ledger grows faster and faster as devices generate large amounts of information and store it within the database. Altered devices are equipped with the ability to alter or delete information. The simulated results depicted the efficiency of the proposed mechanism in the presence of altered devices.

Algorithm 1 Trusted and accurate decision during transmission

1: **Input:** A network 'N' having 'd' number of devices separated into two different categories, i.e., legitimate and malicious
2: **Output:** System is able to take decisions accurately
For each 'd' 1 to 'n' **do**
3: Compute the behavior of each communicating device using the indirect method
4: Call **FEM and Trust Mean Aggregate ()**
5: **if** device 'd' is legitimate **then**
6: FEM

$$T_{complete} = \quad T_{PR} + \quad T_{previous} \tag{12}$$

Where + = 1 depends on specific conditions.
7: Trust Mean Aggregation

$$C_D = \frac{\sum_{s=1}^{n} T_{complete} \quad C_D}{\sum_{s=1}^{n} T_{complete}} \tag{13}$$

8: System can take accurate decisions and predict the surroundings
9: Call **Blockchain ()**
10: **else**
11: device 'd' is malicious
12: **end if**

4. Performance Analysis

To date, the literature in the field has not projected a FEM and blockchain way to analyze the behavior of each device. Here, we have formulated a mathematical trust mean aggregation method to identify the legitimacy of each device. In addition, to analyze the proposed framework, the system is validated on the network having a simulation area of 900 900 using MATLAB considering 25 number of devices.

4.1. Baseline solutions

The proposed mechanism is validated against two conventional approaches proposed by (Huamanchahua et al., 2022; Nguyen et al., 2022). Huamanchahua et al. (Huamanchahua et al., 2022) have reviewed the immersive technology in Industry 4.0. They discussed the implementation aspects and their investigations on various platforms, devices, and software to compact the S3 models. Nguyen et al. (Nguyen et al., 2022) have proposed a Meta-chain blockchain-based architecture for addressing the security concerns of metaverse applications. The proposed framework efficiently managed and automated interactions with their providers and metaverse users. In addition, the authors have used a novel sharing mechanism for improving blockchain scalability. Now, in order to validate the proposed approach with existing approaches, (Huamanchahua et al., 2022) is denoted as Baseline Approach 1 (BA1), (Nguyen et al., 2022) is represented as Baseline Approach 2 (BA2), and the proposed approach is denoted with PA.

4.2. Results and Discussion

The FEM is used for accuracy that is measured through various devices. Each device selects a FEM item $(P_k; D_{k-1})$ to verify and sign the recorded behavior opinion from k device. The resource unit cost $c' = 1$ corresponds to a very low device. In addition, the manufacturing speed and resource cost are directly proportional. The ideal manufacturing process with continuous consumption of resources ensured an efficient and secure communication process. The proposed phenomenon is simulated over broken authentication, eavesdropping, personal information leakage, data injection, and unauthorized access. In addition, depending on the above dataset and the chosen performance metrics, the simulation parameters are defined in Table 2.

Table 2. Simulation environment of the proposed framework.

Parameters	Values
Simulation Time	120s
Devices Type	dynamic
Grid Area	900m 900m
Number of Devices	10-50
Wireless Radio Range	20 mm
Weight values	= 0:6, = 0:4
Rate of compromised IoV	[5; 50]%
Comparisons Protocols	Blockchain, FEM and trust mean aggregate
Devices Type	Legitimate and Altered
Dataset Division	Advertising, Social, Health science
Physical layer	PHY 802.11

Figure 3 depicts the utility comparison among various IoT devices as type 0 (ideal), type 1 (altered), type 2 (highly altered), and type 3 (sensitive). Each device records the behavior using FEM and submits to device for identifying the accuracy of trust prediction. It shows better results compared to existing approaches thanks to the trust-based service composition using FEM.

Figure 4 depicts the eavesdropping while transmitting the information among devices. The proposed mechanism represents the efficiency by applying FEM as

Figure 3. Utility Comparison among Baseline Approaches and Proposed Approach

communicated devices are measured accurately and predicted according to their behavior.

The blockchain integration with FEM provides a transparent and an efficient security solution that resists eavesdropping threats easily compared to existing solutions. The blockchain monitors the entire network and verifies each device on each communication to provide a trusted and secure environment.

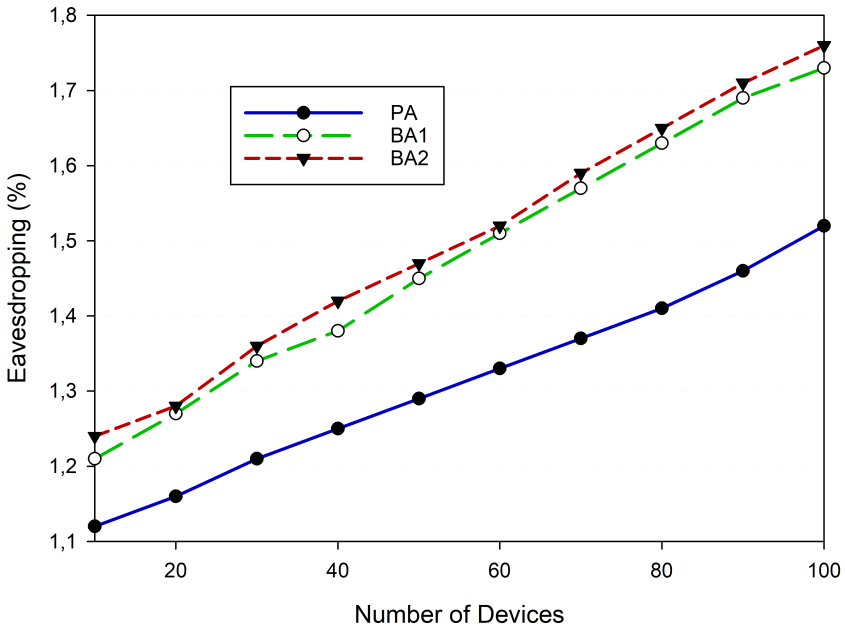

Figure 4. Eavesdropping Comparison between Baseline Approaches and Proposed Approach

Figure 5 presents the personal information leakage graph in which the devices having legitimacy accurately transmit the information where they can be further compromised or altered depending upon time. The proposed framework outperforms the existing approach thanks to the blockchain that inspects and ensures transparency among devices while communicating with each other. A single alteration in information may alter the entire blockchain network and can be easily traced by the remaining devices in the network.

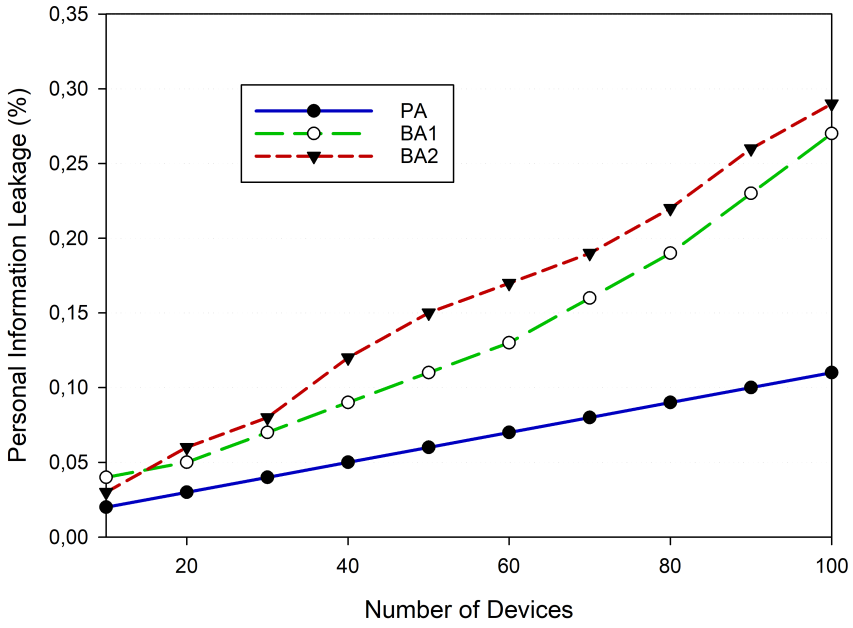

Figure 5. Personal Information Leakage among Baseline Approaches and Proposed Approach

Figure 6 and 7 represent the data injection process and unauthorized access. In depicted Figure 6, the intruders may easily inject malicious information and legitimate data while sharing in the network by compromising the devices. The possibility of data injection in the proposed approach is significantly less compared to existing approaches. In addition, The presented Figure 7 shows that the information can be accessed without authorization in the network using existing approaches compared to the proposed mechanism. The proposed mechanism outperforms the existing phenomenon in both graphs because of the trust mean aggregate and blockchain mechanism process.

4.3. Summary

The security for the industrial communication process considering metaverse applications is validated and verified against trusted schemes such as blockchain and FEM. The proposed approach is validated against utility, eavesdropping, information leakage, and data injection metrics in comparison to conventional approaches. The results of the proposed approach in all the metrics are significant compared to existing approaches. Further, the proposed mechanism significantly measures intruders' alteration during the transmission of information in the network. Any alteration or compromise of legitimate devices can be easily handled and identified at the initial stage of the communication process. The proposed scheme is further analyzed over accuracy rates measured against existing and proposed approaches through a table. The accuracy rates of baselines and proposed algorithms are further presented in Table 3 The out-performance of the proposed mechanism is the integration of fuzzy matrix along with blockchain technology. The fuzzy matrix that computes the legitimacy of each device depending on their trust and internal behavior without increasing the delays and key management overheads in the network. Further,

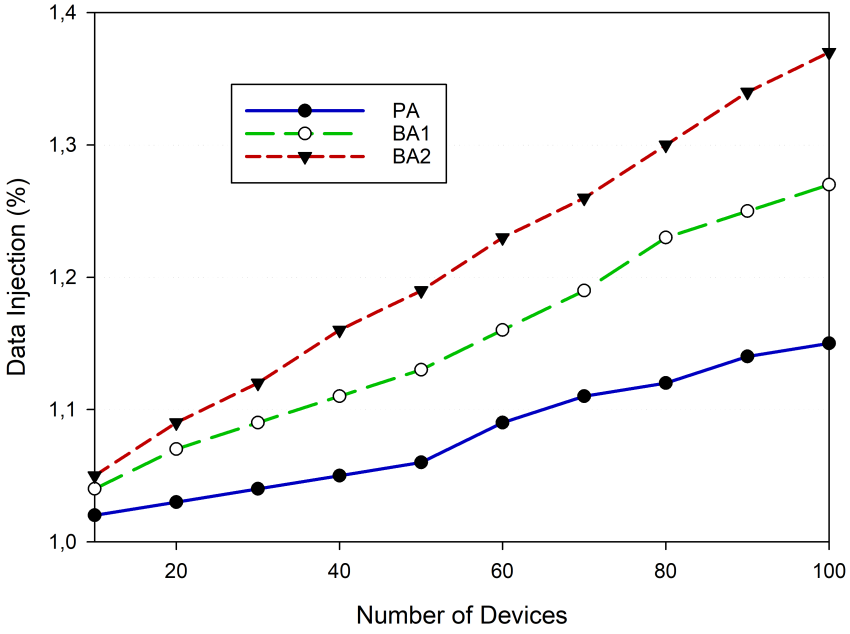

Figure 6. Data Injection Comparison among Baseline Approaches and Proposed Approach

Figure 7. Unauthorized Access Comparison among Baseline Approaches and Proposed Approach

transparency is ensured by providing the blockchain of legitimate devices that keep surveillance and blocked in case of any alteration in the information.

Table 3. Accuracy Percentage

Baseline Approach	Algorithms	Accuracy Percentage
BA1	Software-based S3 model	89%
BA2	Blockchain-based architecture	92%
PA	Blockchain-based FEM	94%

5. Conclusions

This paper aims to propose a secure and efficient blockchain mechanism in Industry 4.0 enabling metaverse environment using fuzzy evaluation matrix (FEM) and trust mean aggregation. The FEM is used for predicting accurate decision-making and analysis of records generated by the system. The proposed mechanism is simulated against various security measures and outperforms different security metrics. The out-performance of the proposed framework compared to the existing methods is due to FEM for accurate decision processes and blockchain mechanism for continuous surveillance. The proposed mechanism showed an approximate 94% improvement in terms of authentication, accuracy, and validation of legitimate devices compared to conventional approaches. Further, besides the real-time testbeds, the dynamic behavior of the mechanism can be further analyzed and measured compared to various security concerns in future works.

References

Anthes, C., Garcıa-Hernández, R. J., Wiedemann, M., & Kranzlmüller, D. (2016). State of the art of virtual reality technology. *2016 IEEE aerospace conference*, 1–19.

Bansal, G., Rajgopal, K., Chamola, V., Xiong, Z., & Niyato, D. (2022). Healthcare in metaverse: A survey on current metaverse applications in healthcare. *Ieee Access*, *10*, 119914–119946.

Chen, Z., Wu, J., Gan, W., & Qi, Z. (2022). Metaverse security and privacy: An overview. *arXiv preprint arXiv:2211.14948*.

Chengoden, R., Victor, N., Huynh-The, T., Yenduri, G., Jhaveri, R. H., Alazab, M., Bhattacharya, S., Hegde, P., Maddikunta, P. K. R., & Gadekallu, T. R. (2023). Metaverse for healthcare: A survey on potential applications, challenges and future directions. *IEEE Access*.

Clim, A. (2019). Cyber security beyond the industry 4.0 era. a short review on a few technological promises. *Informatica Economica*, *23*(2), 34–44.

Fu, Y., Li, C., Yu, F. R., Luan, T. H., Zhao, P., & Liu, S. (2022). A survey of blockchain and intelligent networking for the metaverse. *IEEE Internet of Things Journal*.

Ghobakhloo, M. (2020). Industry 4.0, digitization, and opportunities for sustainability. *Journal of cleaner production*, *252*, 119869.

Guo, D., Li, M., Lyu, Z., Kang, K., Wu, W., Zhong, R. Y., & Huang, G. Q. (2021). Synchroperation in industry 4.0 manufacturing. *International journal of production economics*, *238*, 108171.

Huamanchahua, D., Ricardo, G., Trinidad-Palacios, A. G., Salinas-Bolaños, Y. A., Rosa-Rodrıguez, L. G., & Arancibia-de la Sota, R. A. (2022). The use of immersive technologies in industry 4.0: A state-of-art review. *2022 IEEE ANDESCON*, 1–5.

Huang, Y., Li, Y. J., & Cai, Z. (2023). Security and privacy in metaverse: A comprehensive survey. *Big Data Mining and Analytics*, *6*(2), 234–247.

Kang, J., Xiong, Z., Niyato, D., Xie, S., & Zhang, J. (2019). Incentive mechanism for reliable federated learning: A joint optimization approach to combining reputation and contract theory. *IEEE Internet of Things Journal*, *6*(6), 10700–10714.

Kang, J., Xiong, Z., Niyato, D., Ye, D., Kim, D. I., & Zhao, J. (2019). Toward secure blockchain-enabled internet of vehicles: Optimizing consensus management using reputation and contract theory. *IEEE Transactions on Vehicular Technology*, *68*(3), 2906–2920.

Kim, J. Y., & Oh, J. M. (2022). Opportunities and challenges of metaverse for automotive and mobility industries. *2022 13th International Conference on Information and Communication Technology Convergence (ICTC)*, 113–117.

Kniaziev, S. I. (2017). Development of smart industry as an efficient way to implement the policy of neoindustrialization in the world.

Lakhan, A., Mohammed, M. A., Abdulkareem, K. H., Deveci, M., Marhoon, H. A., Nedoma, J., & Martinek, R. (2024). A multi-objectives framework for secure blockchain in fog-cloud network of vehicle-to-infrastructure applications. *Knowledge-Based Systems*, 111576.

Lakhan, A., Mohammed, M. A., Zebari, D. A., Abdulkareem, K. H., Deveci, M., Marhoon, H. A., Nedoma, J., & Martinek, R. (2024). Augmented iot cooperative vehicular framework based on distributed deep blockchain networks. *IEEE Internet of Things Journal*.

Li, L., Ota, K., & Dong, M. (2018). Deep learning for smart industry: Efficient manufacture inspection system with fog computing. *IEEE Transactions on Industrial Informatics*, *14*(10), 4665–4673.

Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2020). A survey on the security of blockchain systems. *Future generation computer systems*, *107*, 841–853.

Lippert, K., Khan, M. N. R., Rabbi, M. M., Dutta, A., & Cloutier, R. (2021). A framework of metaverse for systems engineering. *2021 IEEE International Conference on Signal Processing, Information, Communication & Systems (SPICSCON)*, 50–54.

Mohammed, M. A., Lakhan, A., Zebari, D. A., Abd Ghani, M. K., Marhoon, H. A., Abdulkareem, K. H., Nedoma, J., & Martinek, R. (2024). Securing healthcare data in industrial cyber-physical systems using combining deep learning and blockchain technology. *Engineering Applications of Arti cial Intelligence*, *129*, 107612.

Mystakidis, S. (2022). Metaverse. *Encyclopedia*, *2*(1), 486–497.

Nguyen, C. T., Hoang, D. T., Nguyen, D. N., & Dutkiewicz, E. (2022). Metachain: A novel blockchain-based framework for metaverse applications. *2022 IEEE 95th Vehicular Technology Conference:(VTC2022-Spring)*, 1–5.

Prinsloo, J., Sinha, S., & von Solms, B. (2019). A review of industry 4.0 manufacturing process security risks. *Applied Sciences*, *9*(23), 5105.

Wang, J., Wang, H., Zhang, H., & Cao, N. (2017). Trust and attribute-based dynamic access control model for internet of things. *2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, 342–345. https://doi.org/10.1109/CyberC.2017.47

Wang, Y., Su, Z., Zhang, N., Xing, R., Liu, D., Luan, T. H., & Shen, X. (2022). A survey on metaverse: Fundamentals, security, and privacy. *IEEE Communications Surveys & Tutorials*.

Wohlgenannt, I., Simons, A., & Stieglitz, S. (2020). Virtual reality. *Business & Information Systems Engineering*, *62*, 455–461.

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2019). Blockchain technology overview. *arXiv preprint arXiv:1906.11078*.

Zonaphan, L., Northus, K., Wijaya, J., Achmad, S., & Sutoyo, R. (2022). Metaverse as a future of education: A systematic review. *2022 8th International HCI and UX Conference in Indonesia (CHIuXiD)*, *1*, 77–81.